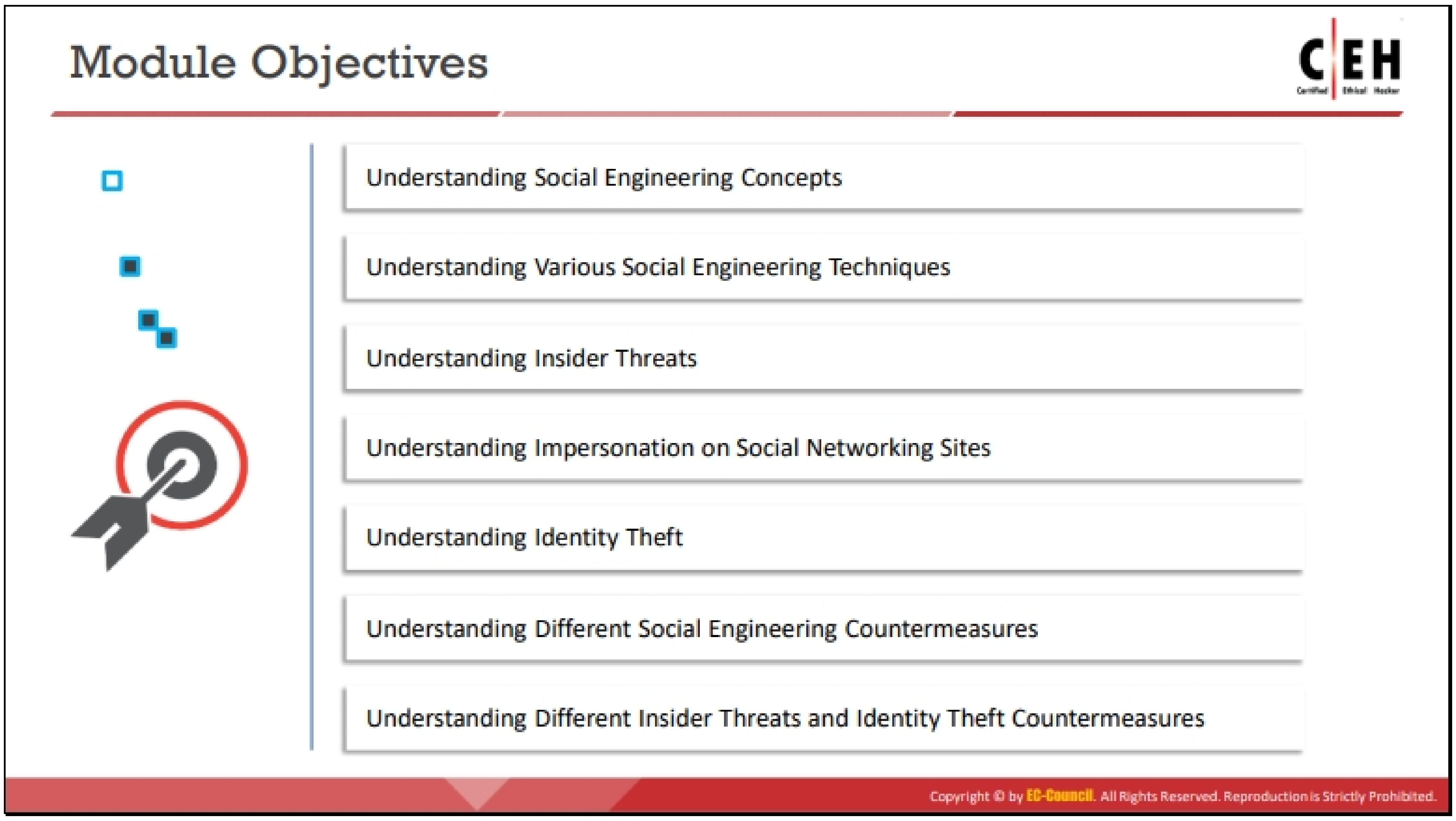
C|EH™

Certified Ethical Hacker

Module 09:

Social Engineering



Module Objectives

- Understanding Social Engineering Concepts
- Understanding Various Social Engineering Techniques
- Understanding Insider Threats
- Understanding Impersonation on Social Networking Sites
- Understanding Identity Theft
- Understanding Different Social Engineering Countermeasures
- Understanding Different Insider Threats and Identity Theft Countermeasures

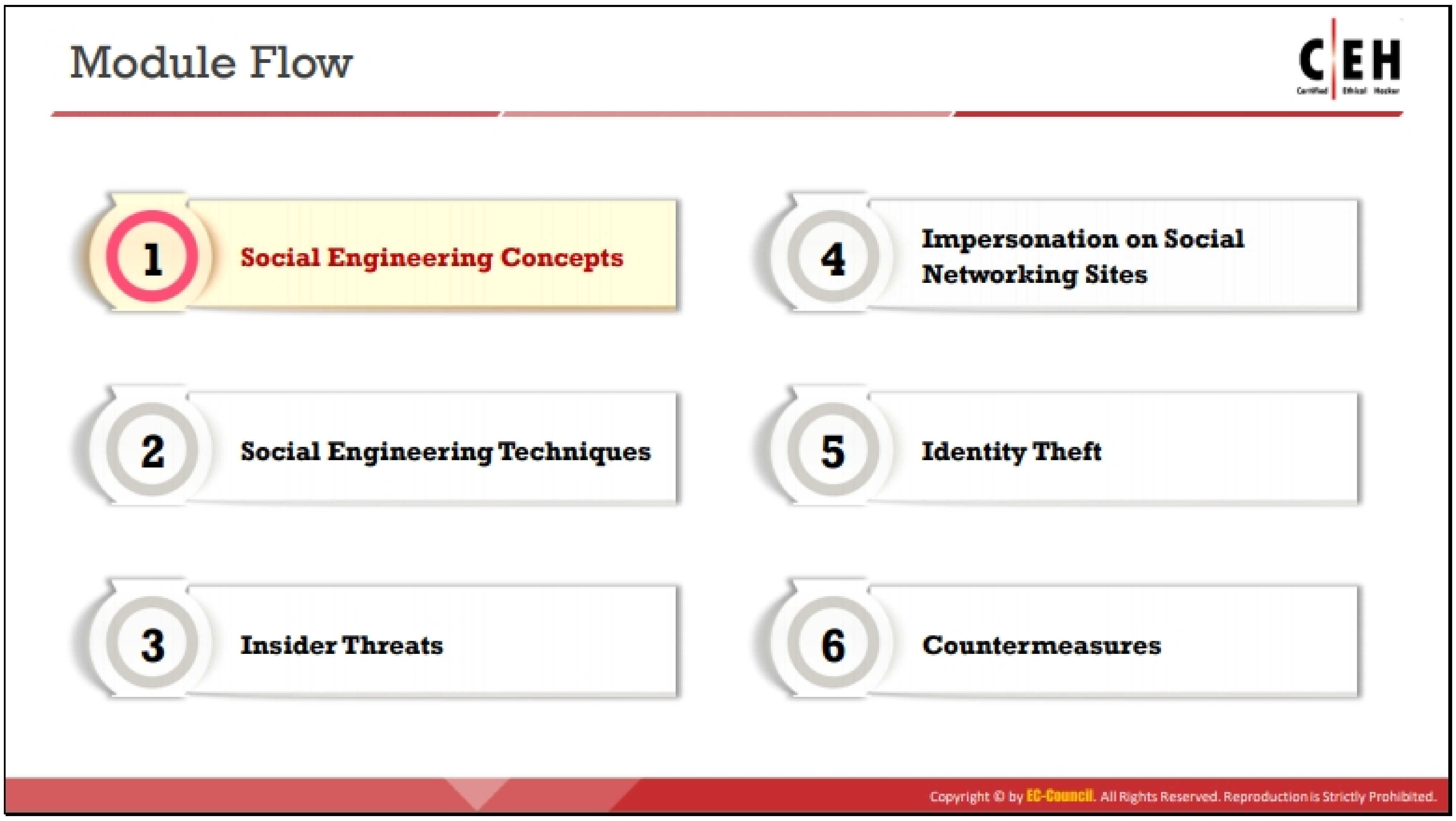
Module Objectives

This module provides an overview of social engineering. Although it focuses on fallacies and advocates effective countermeasures, the possible methods of extracting information from another human being rely on attackers' ingenuity. The features of these techniques make them art, but the psychological nature of some of these techniques makes them a science. The "**bottom line**" is that there is no ready defense against social engineering; only constant vigilance can circumvent some social engineering techniques used by attackers.

This module provides insight into human-based, computer-based, and mobile-based social engineering techniques. It also discusses various insider threats — impersonation on social networking sites, identity theft, as well as possible countermeasures.

At the end of this module, you will be able to:

- Describe social engineering concepts
- Perform social engineering using various techniques
- Describe insider threats
- Perform impersonation on social networking sites
- Describe identity theft
- Apply social engineering countermeasures
- Apply knowledge of insider threats and identity theft countermeasures



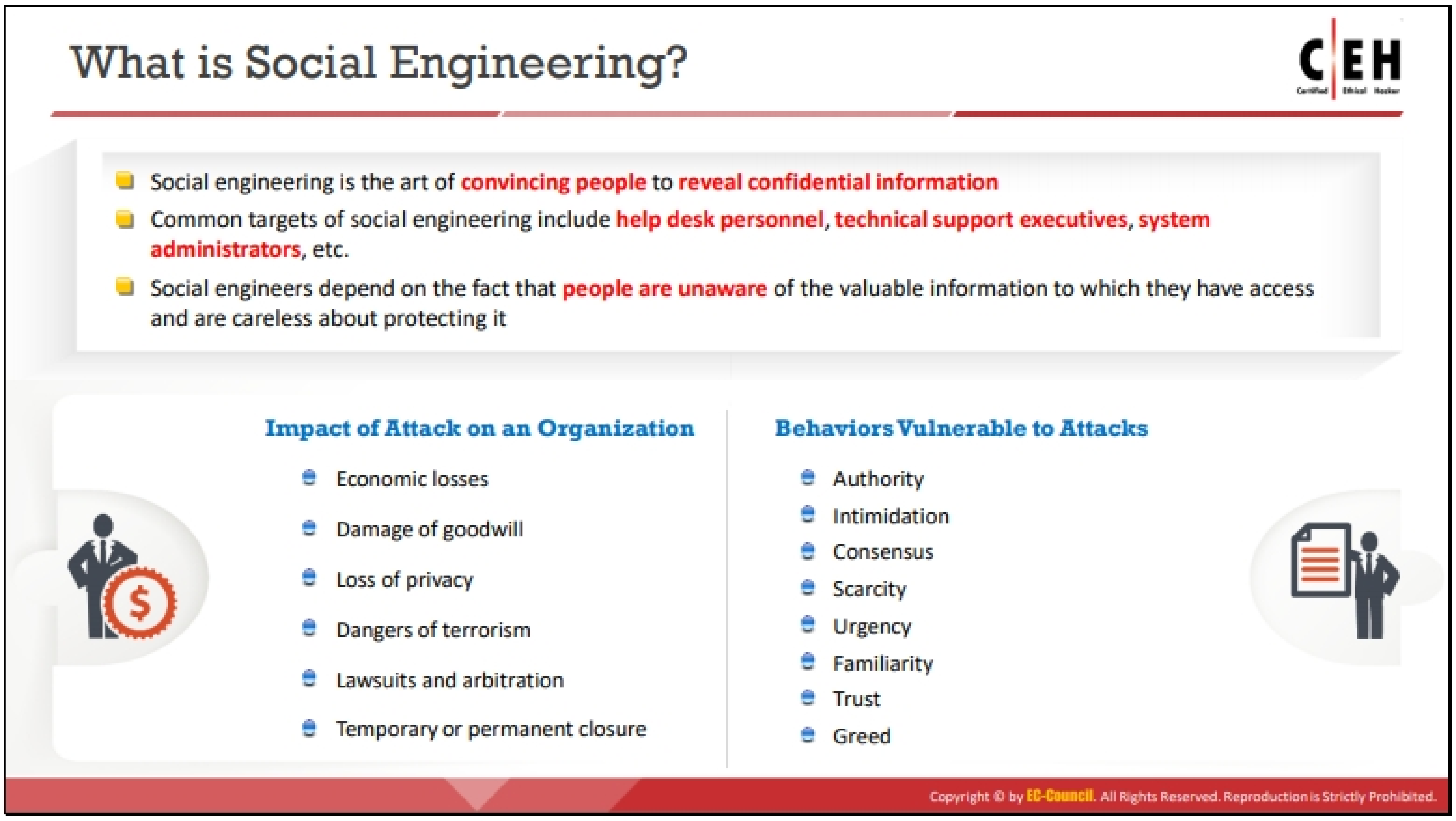
Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures

Social Engineering Concepts

There is no single security mechanism that can protect from the social engineering techniques used by attackers. Only educating employees on how to recognize and respond to social engineering attacks can minimize attackers' chances of success. Before going ahead with this module, it is first necessary to discuss various social engineering concepts.

This section describes social engineering, frequent targets of social engineering, behaviors vulnerable to attack, factors making companies vulnerable to attack, why social engineering is effective, the principles of social engineering, and the phases of a social engineering attack.



What is Social Engineering?

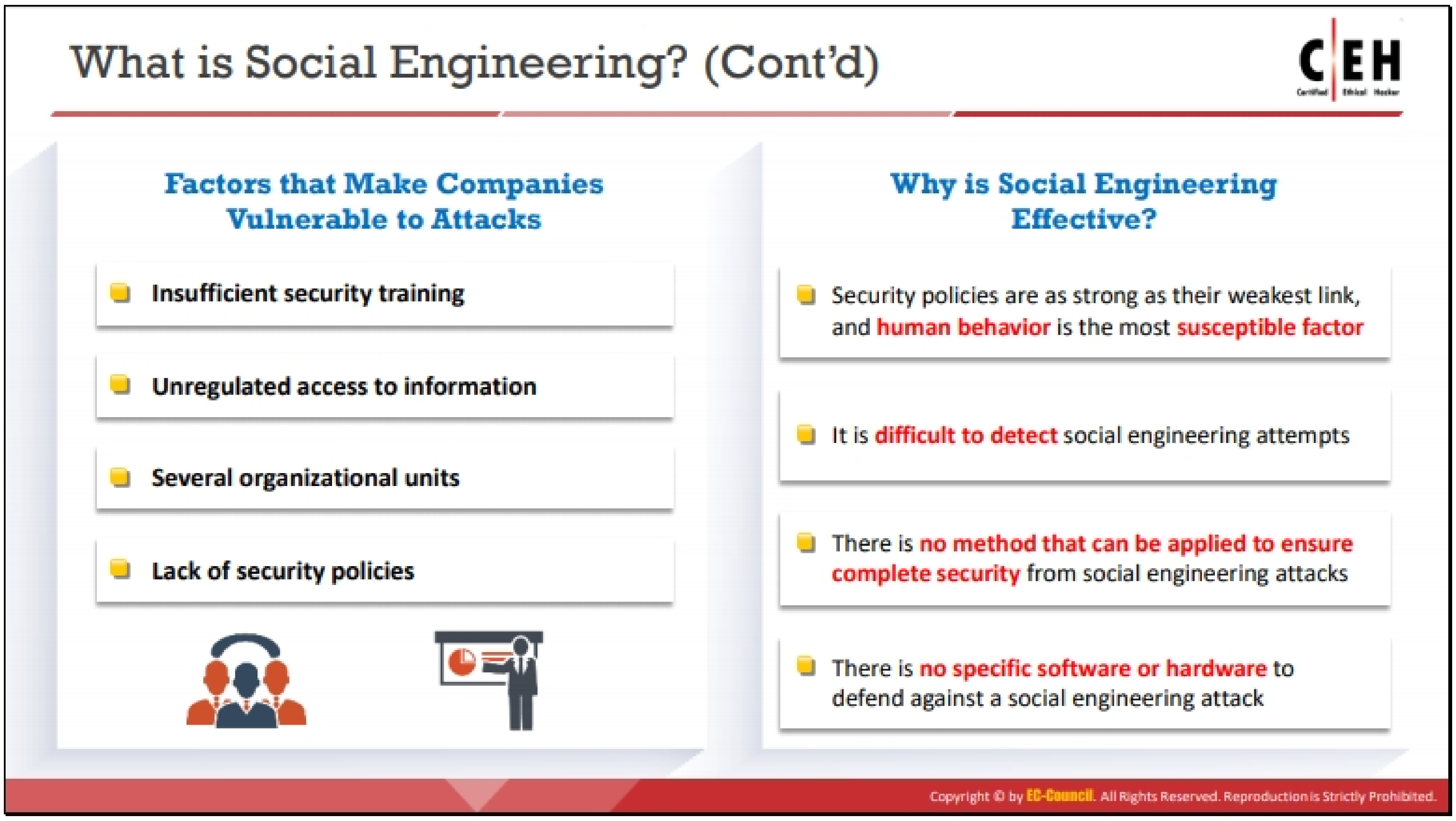
- Social engineering is the art of **convincing people** to **reveal confidential information**
- Common targets of social engineering include **help desk personnel**, **technical support executives**, **system administrators**, etc.
- Social engineers depend on the fact that **people are unaware** of the valuable information to which they have access and are careless about protecting it

Impact of Attack on an Organization

- Economic losses
- Damage of goodwill
- Loss of privacy
- Dangers of terrorism
- Lawsuits and arbitration
- Temporary or permanent closure

Behaviors Vulnerable to Attacks

- Authority
- Intimidation
- Consensus
- Scarcity
- Urgency
- Familiarity
- Trust
- Greed



What is Social Engineering? (Cont'd)

Factors that Make Companies Vulnerable to Attacks

- **Insufficient security training**
- **Unregulated access to information**
- **Several organizational units**
- **Lack of security policies**

Why is Social Engineering Effective?

- Security policies are as strong as their weakest link, and **human behavior** is the most **susceptible factor**
- It is **difficult to detect** social engineering attempts
- There is **no method that can be applied to ensure complete security** from social engineering attacks
- There is **no specific software or hardware** to defend against a social engineering attack

What is Social Engineering?

Before performing a social engineering attack, the attacker gathers information about the target organization from various sources such as:

- The organization's official websites, where employees' IDs, names, and email addresses are shared

- Advertisements of the target organization cast through media reveal information such as products and offers.
- Blogs, forums, and other online spaces where employees share basic personal and organizational information.

After gathering information, an attacker executes social engineering attacks using various approaches such as impersonation, piggybacking, tailgating, reverse social engineering, and other methods.

Social engineering is the art of manipulating people to divulge sensitive information to use it to perform some malicious action. Despite security policies, attackers can compromise an organization's sensitive information by using social engineering, which targets the weakness of people. Most often, employees are not even aware of a security lapse on their part and inadvertently reveal the organization's critical information. For instance, unwittingly answering strangers' questions or replying to spam email.

To succeed, attackers take a special interest in developing social engineering skills and can be so proficient that the victims might not even notice the fraud. Attackers always look for new ways to access information. They also ensure that they know the organization's perimeter and the people on its **perimeter**, such as security guards, receptionists, and help-desk workers, to exploit human oversight. People have conditioned themselves to not be overly suspicious, and they associate specific behaviors and appearances with known entities. For instance, a man in a uniform carrying a pile of packages for delivery will be perceived as a delivery person. With the help of social engineering tricks, attackers succeed in obtaining confidential information, authorization, and access details from people by deceiving and manipulating human vulnerability.

Common Targets of Social Engineering

A social engineer uses the vulnerability of human nature as their most effective tool. Usually, people believe and trust others and derive fulfillment from helping the needy. Discussed below are the most common targets of social engineering in an organization:

- **Receptionists and Help-Desk Personnel**: Social engineers generally target service-desk or help-desk personnel by tricking them into divulging confidential information about the organization. To extract information, such as a phone number or password, the attacker first wins the trust of the individual with the information. On winning their trust, the attacker manipulates them to get valuable information. Receptionists and help-desk staff may readily share information if they feel they are doing so to help a customer.
- **Technical Support Executives**: Another target of social engineers is technical support executives. The social engineers may take the approach of contacting technical support executives to obtain sensitive information by pretending to be senior management, customers, vendors, or other figures.
- **System Administrators**: A system administrator in an organization is responsible for maintaining the systems. Thus, they may have critical information such as the type and

version of OS and admin passwords, that could be helpful for an attacker in planning an attack.

- **Users and Clients**: Attackers could approach users and clients of the target organization, pretending to be a tech support person to extract sensitive information.
- **Vendors of the Target Organization**: Attackers may also target the vendors of the organization to gain critical information that could help in executing attacks.
- **Senior Executives:** Attackers could also approach senior executives from various departments such as Finance, HR, and CxOs to obtain critical information about the organization

Impact of Social Engineering Attack on an Organization

Social engineering does not seem like a serious threat, but it can lead to substantial losses for organizations. The impact of social engineering attack on organizations include:

- **Economic Losses**: Competitors may use social engineering techniques to steal sensitive information such as the development plans and marketing strategies of the target company, which can result in an economic loss.
- **Damage to Goodwill**: For an organization, goodwill is important for attracting customers. Social engineering attacks may damage that goodwill by leaking sensitive organizational data.
- **Loss of Privacy**: Privacy is a major concern, especially for big organizations. If an organization is unable to maintain the privacy of its stakeholders or customers, then people can lose trust in the company and may discontinue their business association with the organization. Consequently, the organization could face losses.
- **Dangers of Terrorism**: Terrorism and anti-social elements pose a threat to an organization's assets — people and property. Terrorists may use social engineering techniques to make blueprints of their targets to infiltrate their targets.
- **Lawsuits and Arbitration**: Lawsuits and arbitration result in negative publicity for an organization and affects the business's performance.
- **Temporary or Permanent Closure**: Social engineering attacks can result in a loss of goodwill. Lawsuits and arbitration may force the temporary or permanent closure of an organization and its business activities.

Behaviors Vulnerable to Attacks

- **Authority**

  Authority implies the right to exercise power in an organization. Attackers take advantage of this by presenting themselves as a person of authority, such as a technician or an executive, in a target organization to steal important data.

  For example, an attacker can call a user on the phone and can claim to be working as a network administrator in the target organization. The attacker then informs the victim about a security incident in the network and asks them to provide their account credentials to protect their data against theft. After obtaining the victim's credentials, the attacker steals sensitive information from the victim's account.

- **Intimidation**

  Intimidation refers to an attempt to intimidate a victim into taking several actions by using bullying tactics. It is usually performed by impersonating some other person and manipulating users into disclosing sensitive information.

  For example, an attacker might call the executive's receptionist with this request:

  "Mr. Tibiyani is about to give a big presentation to the customers, but he is unable to open his files; it seems they are corrupt. He told me to call you and ask you to send the files to me immediately so that he can start his talk."

- **Consensus or Social Proof**

  Consensus or social proof refers to the fact that people are usually willing to like things or do things that other people like or do.

  Attackers take advantage of this by doing things like creating websites and posting fake testimonials from users about the benefits of certain products such as anti-malware (rogueware). Therefore, if users search the Internet to download the rogueware, they encounter these websites and believe the forged testimonials. Further, if users download the malicious product, attackers may install a trojan along with it.

- **Scarcity**

  Scarcity implies the state of being scarce. In the context of social engineering, scarcity often implies creating a feeling of urgency in a decision-making process. Due to this urgency, attackers can control the information provided to victims and manipulate the decision-making process.

  For example, when Apple releases a new iPhone product that sells out and goes out of stock, attackers can take advantage of this situation by sending a phishing email to the target users, encouraging them to click on a link provided in the email to buy the product. If the users click on this link, they get redirected to some malicious website controlled by the attacker. As a result, the user might end up revealing their account details or downloading some malicious programs such as trojans.

- **Urgency**

  Urgency implies encouraging people to take immediate action. Attackers can take advantage of this by tricking victims into performing unintended tasks.

  For example, ransomware often uses the urgency principle, which makes the victim take urgent action under a time-limit. The victims see the countdown timer running on their infected systems and know that failure to make the required decision within the given time can result in the loss of important data.

  Similarly, attackers can send phishing emails indicating that a certain product is available at a low price and that to buy it, the user should click on the "Buy Now" link. The user is tricked, and they click on the link to take immediate action. As a result, they are redirected to a malicious website and end up revealing their account details or downloading a virus file.

- **Familiarity or Liking**

  Familiarity or liking implies that people are more likely to be persuaded to do something when they are asked by someone whom they like. This indicates that people are more likely to buy products if they are advertised by an admired celebrity.

  For example, people are more likely to allow someone to look over their shoulder if they like that person or they are familiar with them. If people do not like the person, they immediately recognize the shoulder surfing attack and prevent it. Similarly, people often allow someone to tailgate them if they like that person or are familiar with them. In some cases, social engineers use a charming smile and sweet-talk to deceive the other person into liking them.

- **Trust**

  Attackers often attempt to build a trusting relationship with victims.

  For example, an attacker can call a victim and introduce themself as a security expert. Then, they may claim that they were working with XYZ company, and they noticed some unusual errors sent from the victim's system. The attacker builds trust by using the company name and their experience in the security field. After establishing trust, the attacker guides the victim to follow a series of steps to "view and disable the system errors." They later send an email containing a malicious file and persuade the victim to click on and download it. Through this process, the attacker successfully installs malware on the victim's system, infecting it and allowing the attacker to steal important information.

- **Greed**

  Some people are possessive by nature and seek to acquire vast amounts of wealth through illegal activities. Social engineers lure their targets to divulge information by promising something for nothing (appealing to their greed).

  For example, an attacker may pretend to be a competitor and lure the employees of the target into revealing critical information by offering a considerable reward.

Factors that Make Companies Vulnerable to Attacks

Many factors make companies vulnerable to social engineering attacks; some of them are as follows:

- **Insufficient Security Training**

  Employees can be ignorant about the social engineering tricks used by attackers to lure them into divulging sensitive data about the organization. Therefore, the minimum responsibility of any organization is to educate their employees about social engineering techniques and the threats associated with them to prevent social engineering attacks.

- **Unregulated Access to Information**

  For any company, one of its main assets is its database. Providing unlimited access or allowing everyone access to such sensitive data might cause trouble. Therefore, companies must ensure proper training for and surveillance of key personnel accessing sensitive data.

- **Several Organizational Units**

  Some organizations have their units at different geographic locations, making it difficult to manage the system. Further, this sort of setup makes it easier for an attacker to access the organization's sensitive information.

- **Lack of Security Policies**

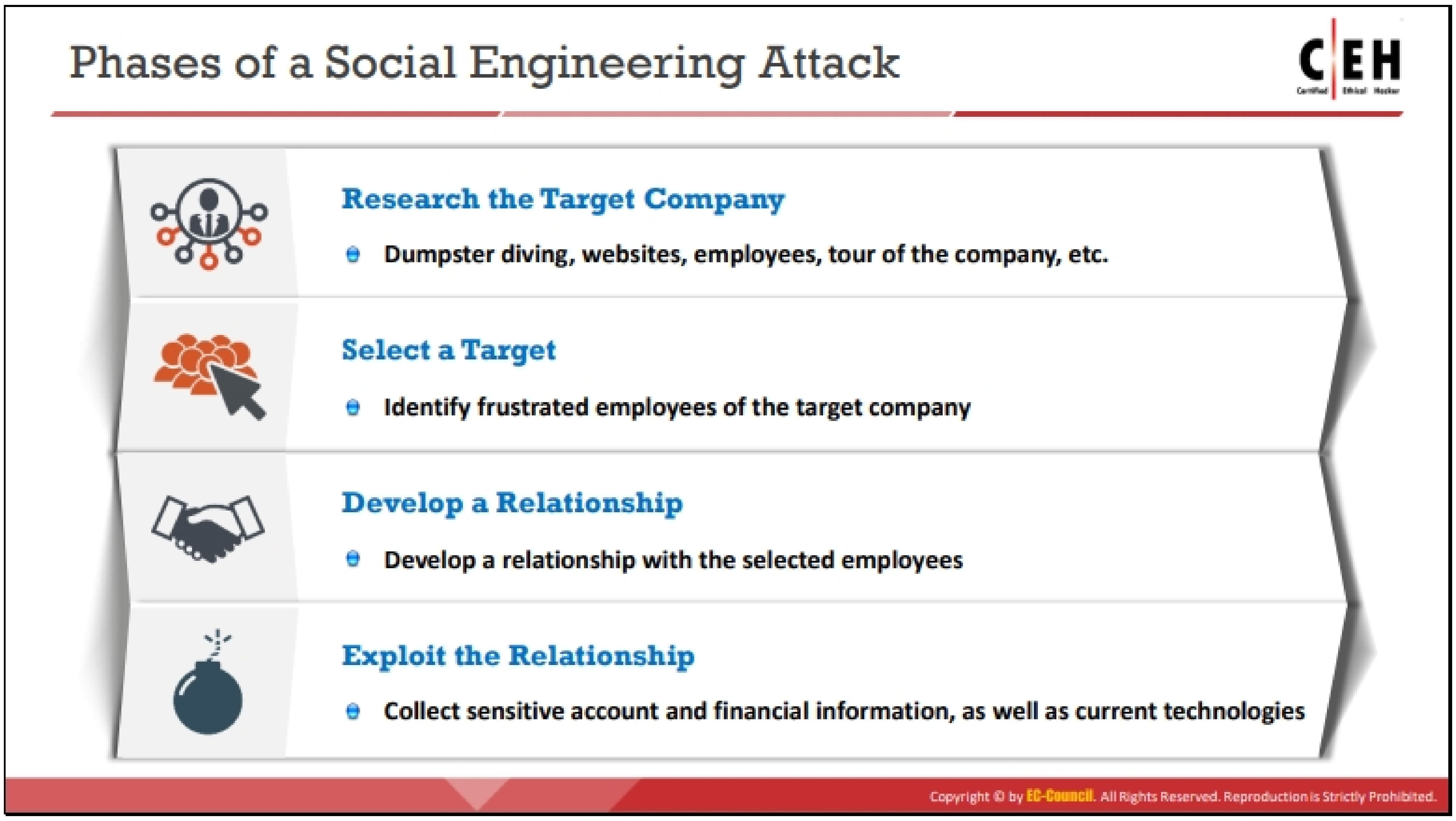
  Security policy is the foundation of security infrastructure. It is a high-level document describing the security controls implemented in a company. An organization should take extreme measures related to every possible security threat or vulnerability. Implementation of certain security measures such as password change policy, information sharing policy, access privileges, unique user identification, and centralized security, prove to be beneficial.

Why is Social Engineering Effective?

Like other techniques, social engineering does not deal with network security issues; instead, it deals with the psychological manipulation of a human being to extract desired information.

The following are reasons why social engineering continues to be effective:

- Despite various security policies, preventing social engineering is a challenge because human beings are most susceptible to variation.
- It is challenging to detect social engineering attempts. Social engineering is the art and science of manipulating people into divulging information.
- No method guarantees complete security from social engineering attacks.
- No specific hardware or software is available to safeguard against social engineering attacks.
- This approach is relatively cheap (or free) and easy to implement.



Phases of a Social Engineering Attack

Research the Target Company

- Dumpster diving, websites, employees, tour of the company, etc.

Select a Target

- Identify frustrated employees of the target company

Develop a Relationship

- Develop a relationship with the selected employees

Exploit the Relationship

- Collect sensitive account and financial information, as well as current technologies

Phases of a Social Engineering Attack

Attackers take the following steps to execute a successful social engineering attack:

- **Research the Target Company**

  Before attacking the target organization's network, an attacker gathers enough information to infiltrate the system. Social engineering is one technique that helps in extracting information. Initially, the attacker researches basic information about the target organization, such as the nature of the business, its location, number of employees, and other facts. While researching, the attacker indulges in activities such as dumpster diving, browsing the company's website, and finding employee details.

- **Select a Target**

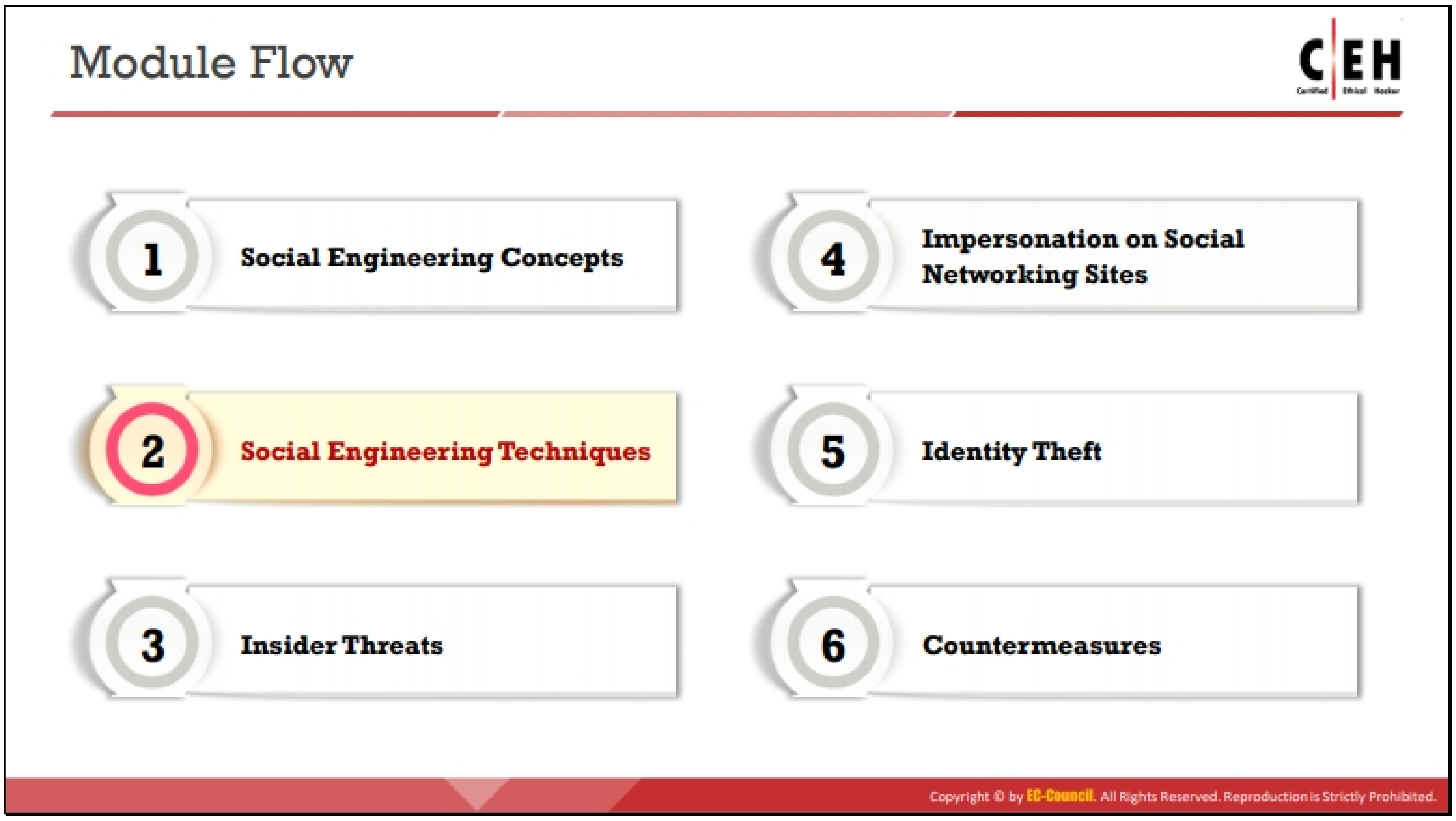
  After finishing their research, the attacker selects a target for extracting sensitive information about the organization. Usually, attackers try to reach out to disgruntled employees because they are easier to manipulate.

- **Develop a Relationship**

  Once the target is set, the attacker builds a relationship with that employee to accomplish their task.

- **Exploit the Relationship**

  The attacker exploits the relationship and extracts sensitive information about the organization's accounts, finance information, technologies in use, and upcoming plans.



Module Flow

1 Social Engineering Concepts

2 Social Engineering Techniques

3 Insider Threats

4 Impersonation on Social Networking Sites

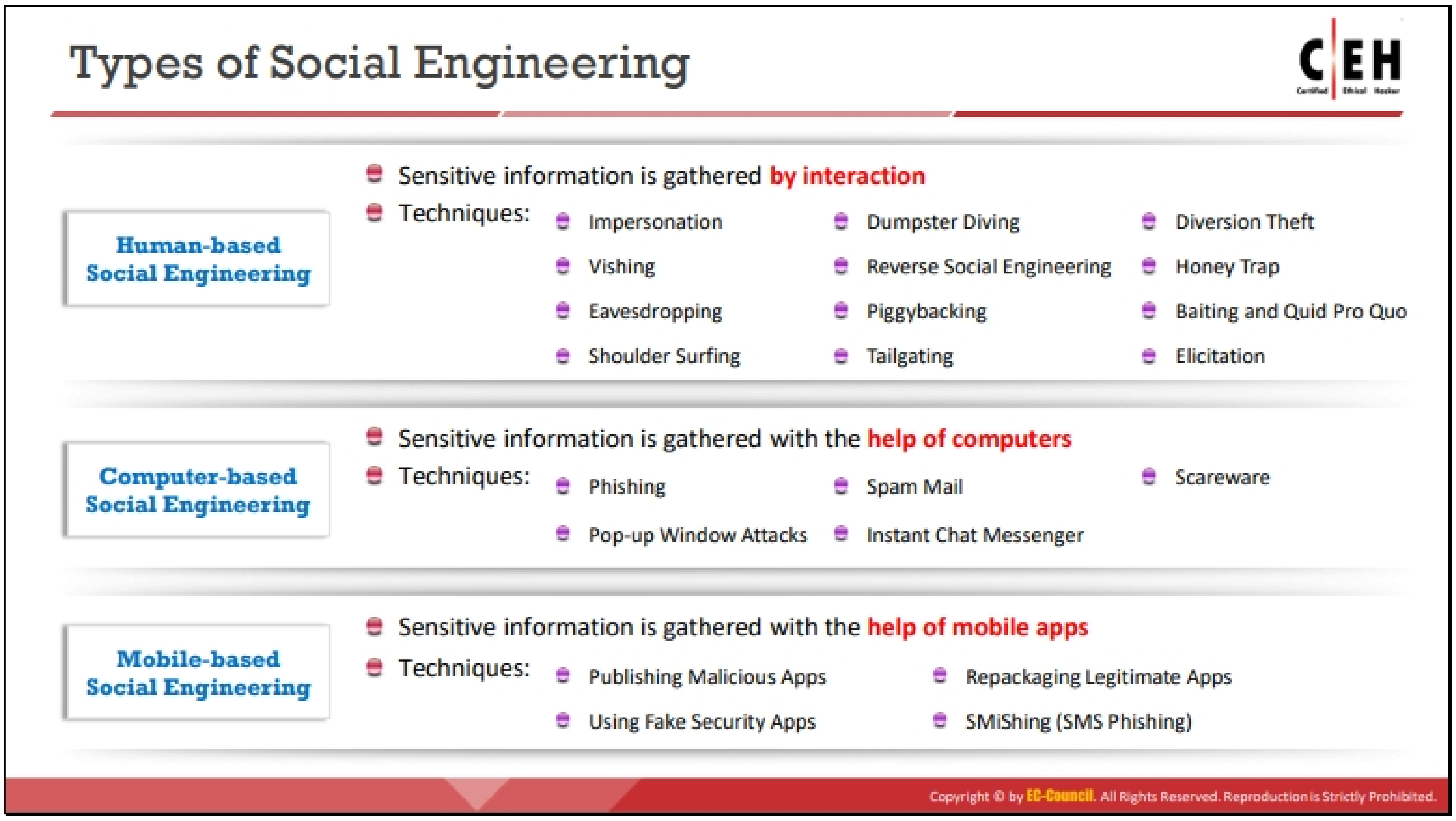
5 Identity Theft

6 Countermeasures

Social Engineering Techniques

Attackers implement various social engineering techniques to gather sensitive information from people or organizations that might help them to commit fraud or participate in other criminal activities.

This section deals with various human-based, computer-based, and mobile-based social engineering techniques, coded with examples for a better understanding.



Types of Social Engineering

Human-based Social Engineering

- Sensitive information is gathered **by interaction**
- Techniques:
  - Impersonation
  - Vishing
  - Eavesdropping
  - Shoulder Surfing
  - Dumpster Diving
  - Reverse Social Engineering
  - Piggybacking
  - Tailgating
  - Diversion Theft
  - Honey Trap
  - Baiting and Quid Pro Quo
  - Elicitation

Computer-based Social Engineering

- Sensitive information is gathered with the **help of computers**
- Techniques:
  - Phishing
  - Pop-up Window Attacks
  - Spam Mail
  - Instant Chat Messenger
  - Scareware

Mobile-based Social Engineering

- Sensitive information is gathered with the **help of mobile apps**
- Techniques:
  - Publishing Malicious Apps
  - Using Fake Security Apps
  - Repackaging Legitimate Apps
  - SMiShing (SMS Phishing)

Types of Social Engineering

In a social engineering attack, the attacker uses their social skills to trick the victim into disclosing personal information such as credit card numbers, bank account numbers, and phone numbers, or confidential information about their organization or computer system. Attackers use this data to either launch an attack or to commit fraud. Social engineering attacks are categorized into three categories: human-based, computer-based, and mobile-based.

- **Human-based Social Engineering**

  Human-based social engineering involves human interaction. Acting as though they were a legitimate person, the attacker interacts with the employee of the target organization to collect sensitive information, such as business plans and networks, that might help them in launching their attack. For example, impersonating an IT support technician, the attacker can easily access the server room.

  An attacker can perform human-based social engineering by using the following techniques:

  - Impersonation
  - Vishing
  - Eavesdropping
  - Shoulder Surfing
  - Dumpster Diving
  - Reverse Social Engineering
  - Piggybacking
  - Tailgating
  - Diversion Theft
  - Honey Trap
  - Baiting
  - Quid Pro Quo
  - Elicitation

- **Computer-based Social Engineering**

  Computer-based social engineering relies on computers and Internet systems to carry out the targeted action.

  The following techniques can be used for computer-based social engineering:

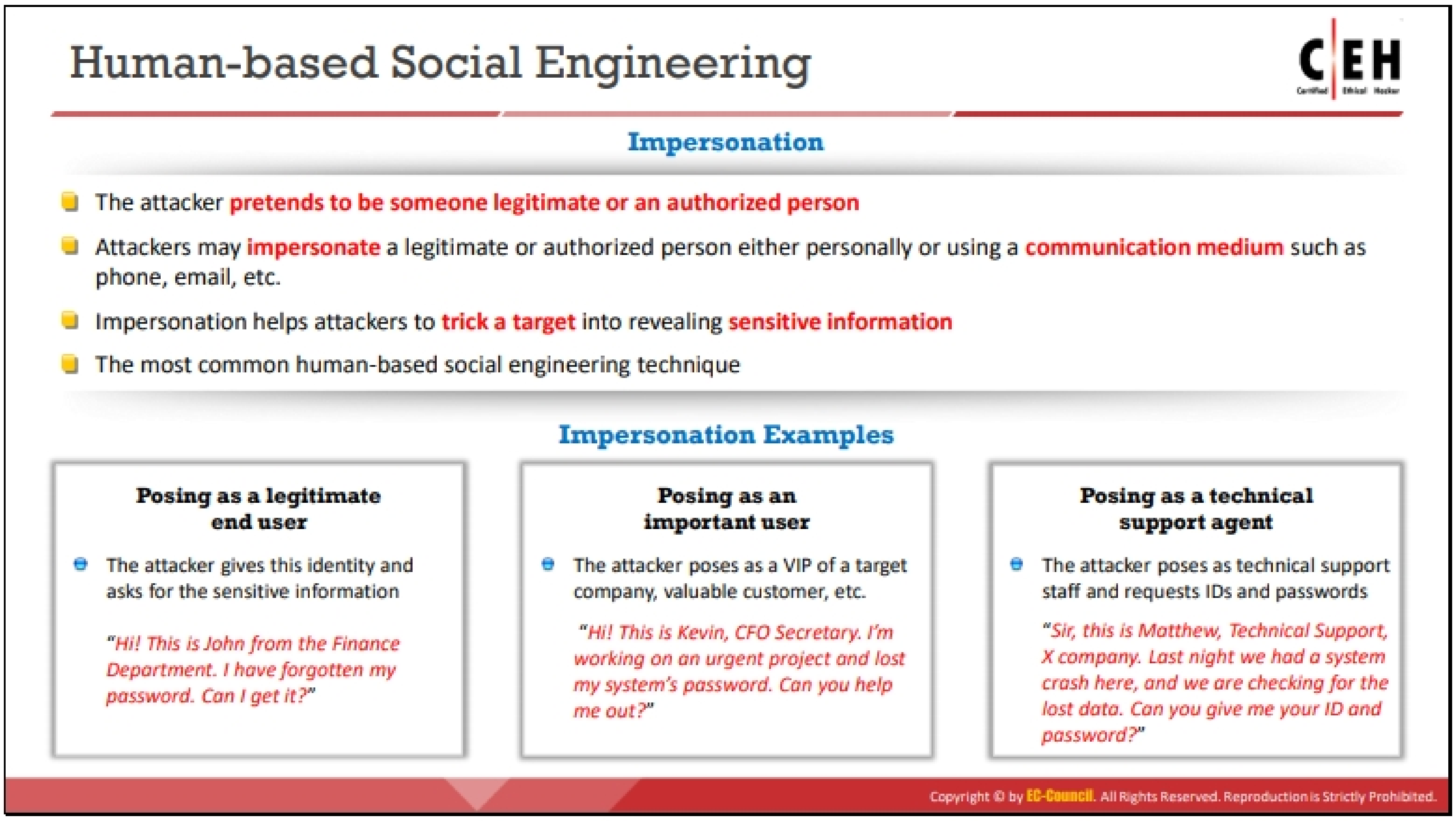
  - Phishing
  - Spam mail
  - Instant chat messenger
  - Pop-up window attacks
  - Scareware

- **Mobile-based Social Engineering**

  Attackers use mobile applications to carry out mobile-based social engineering. Attackers trick the users by imitating popular applications and creating malicious mobile applications with attractive features and submitting them to the major app stores with the same name. Users unknowingly download the malicious app, allowing the malware to infect their device.

  Listed below are some techniques attackers use to perform mobile-based social engineering:

  - Publishing malicious apps
  - Repackaging legitimate apps
  - Using fake security applications
  - SMiShing (SMS Phishing)



Human-based Social Engineering

Impersonation

- The attacker **pretends to be someone legitimate or an authorized person**
- Attackers may **impersonate** a legitimate or authorized person either personally or using a **communication medium** such as phone, email, etc.
- Impersonation helps attackers to **trick a target** into revealing **sensitive information**
- The most common human-based social engineering technique

Impersonation Examples

Posing as a legitimate end user

- The attacker gives this identity and asks for the sensitive information

"Hi! This is John from the Finance Department. I have forgotten my password. Can I get it?"

Posing as an important user

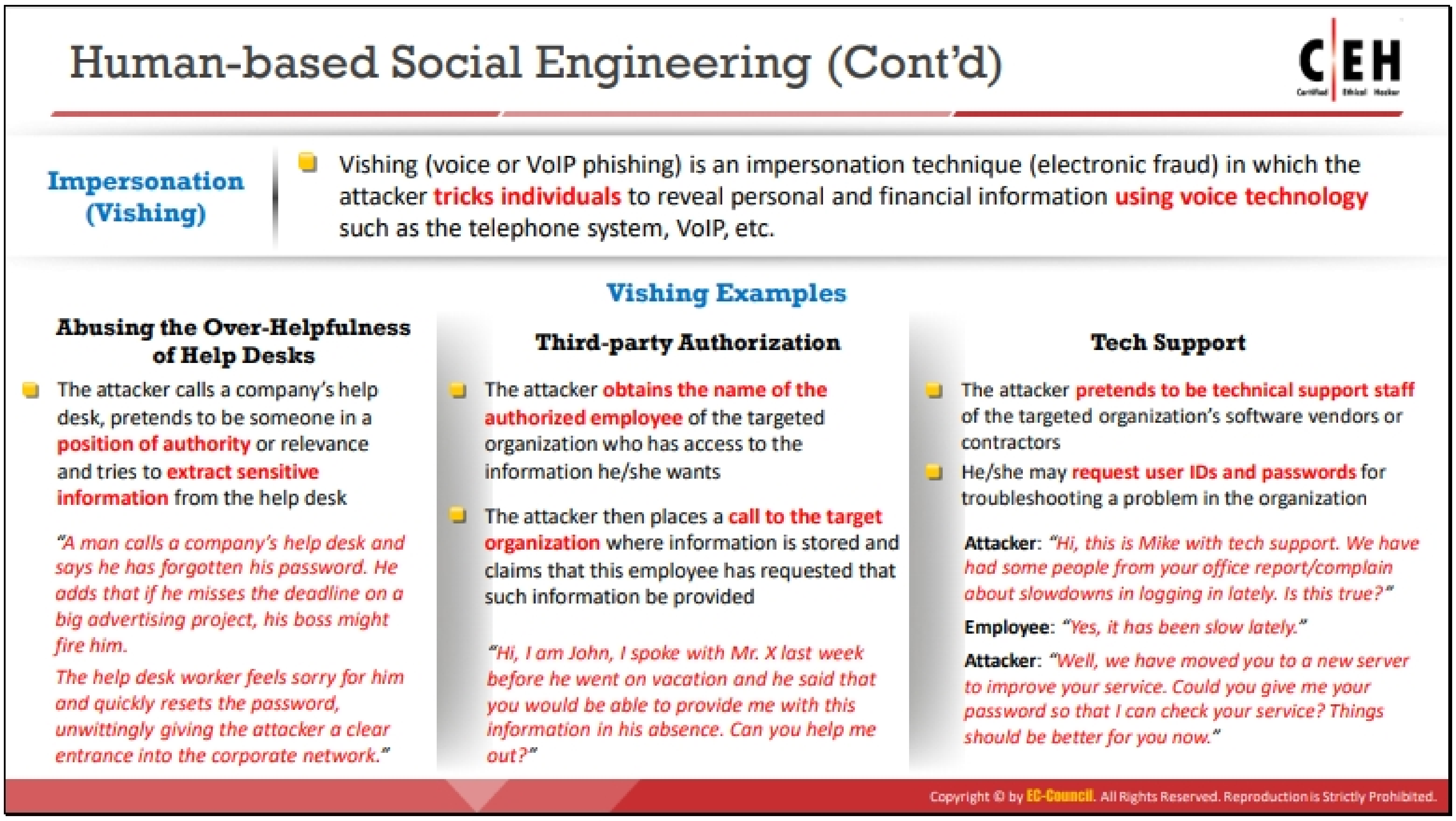
- The attacker poses as a VIP of a target company, valuable customer, etc.

"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system's password. Can you help me out?"

Posing as a technical support agent

- The attacker poses as technical support staff and requests IDs and passwords

"Sir, this is Matthew, Technical Support, X company. Last night we had a system crash here, and we are checking for the lost data. Can you give me your ID and password?"



Human-based Social Engineering (Cont'd)

Impersonation (Vishing)

- Vishing (voice or VoIP phishing) is an impersonation technique (electronic fraud) in which the attacker **tricks individuals** to reveal personal and financial information **using voice technology** such as the telephone system, VoIP, etc.

Vishing Examples

Abusing the Over-Helpfulness of Help Desks

- The attacker calls a company's help desk, pretends to be someone in a **position of authority** or relevance and tries to **extract sensitive information** from the help desk

"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker a clear entrance into the corporate network."

Third-party Authorization

- The attacker **obtains the name of the authorized employee** of the targeted organization who has access to the information he/she wants
- The attacker then places a **call to the target organization** where information is stored and claims that this employee has requested that such information be provided

"Hi, I am John, I spoke with Mr. X last week before he went on vacation and he said that you would be able to provide me with this information in his absence. Can you help me out?"

Tech Support

- The attacker **pretends to be technical support staff** of the targeted organization's software vendors or contractors
- He/she may **request user IDs and passwords** for troubleshooting a problem in the organization

Attacker: *"Hi, this is Mike with tech support. We have had some people from your office report/complain about slowdowns in logging in lately. Is this true?"*

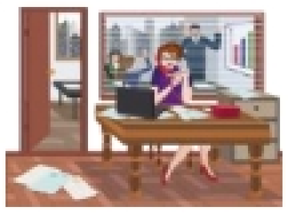
Employee: *"Yes, it has been slow lately."*

Attacker: *"Well, we have moved you to a new server to improve your service. Could you give me your password so that I can check your service? Things should be better for you now."*

Human-based Social Engineering (Cont'd)

Eavesdropping

- **Unauthorized listening of conversations**, or reading of messages
- Interception of audio, video, or written communication
- Can be done using **communication channels** such as telephone lines, email, instant messaging, etc.

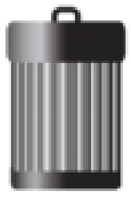


Shoulder Surfing

- Direct observation techniques such as **looking over someone's shoulder** to get information such as passwords, PINs, account numbers, etc.
- Can also be done from a farther distance with the aid of **vision enhancing devices** such as binoculars

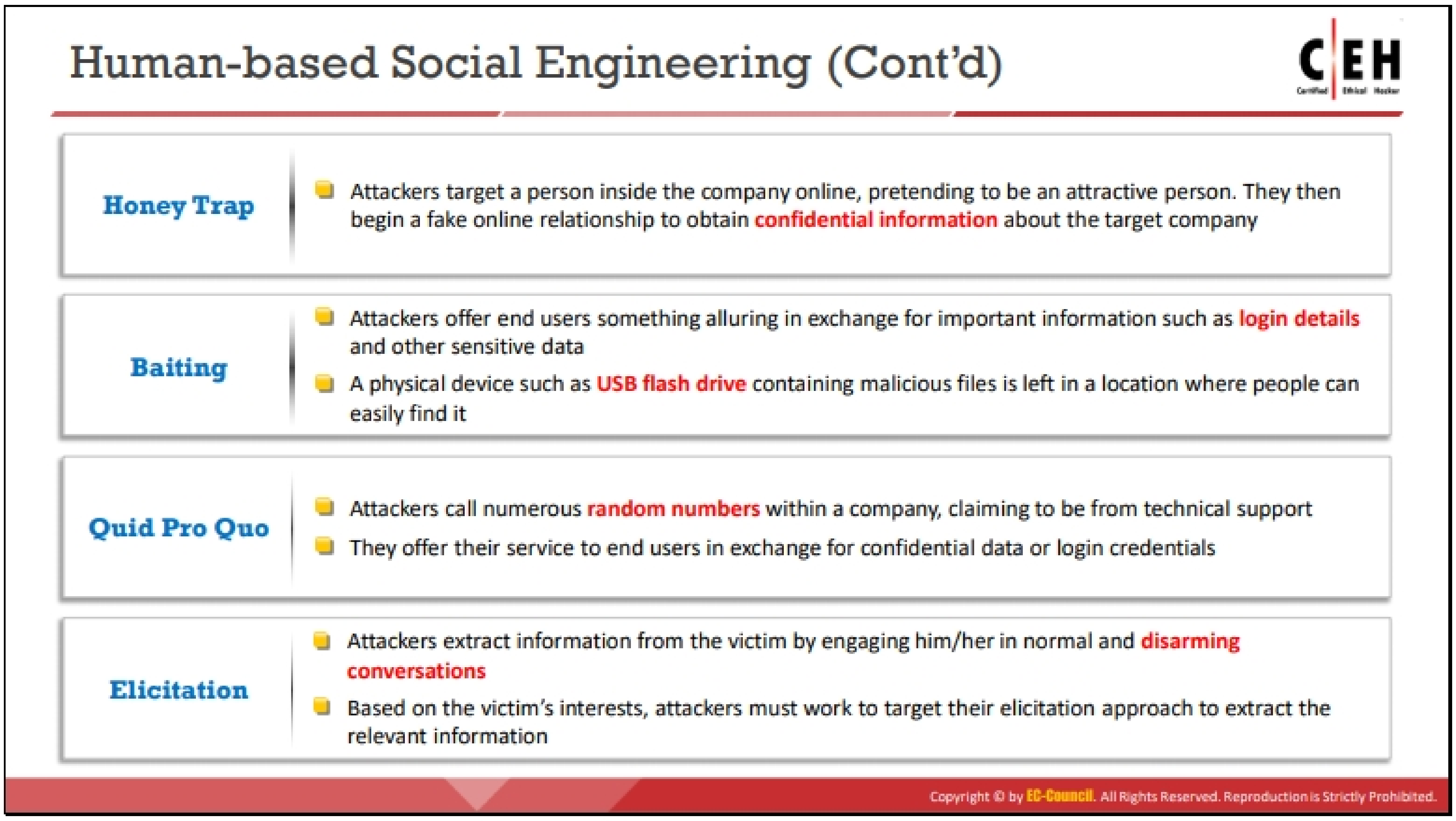
Dumpster Diving

- **Looking for treasure in someone else's trash**
- Involves collecting **phone bills**, **contact information**, **financial information**, operations-related information, etc. from the target company's trash bins or printer bins, or user desks (e.g., sticky notes), etc.



Human-based Social Engineering (Cont'd)

Reverse Social Engineering	The attacker presents him/herself as an **authority** and the target seeks his or her advice before or after offering the information that the attacker needs
Piggybacking	An authorized person intentionally or unintentionally allows an **unauthorized person** to pass through a secure door e.g., "I forgot my ID badge at home. Please help me"
Tailgating	The attacker, wearing a **fake ID badge**, enters a secured area by closely following an authorized person through a door that requires key access
Diversion Theft	The attacker **tricks a person responsible for making a genuine delivery** into delivering the consignment to a location other than the intended location



Human-based Social Engineering (Cont'd)

Honey Trap	Attackers target a person inside the company online, pretending to be an attractive person. They then begin a fake online relationship to obtain **confidential information** about the target company
Baiting	Attackers offer end users something alluring in exchange for important information such as **login details** and other sensitive data A physical device such as **USB flash drive** containing malicious files is left in a location where people can easily find it
Quid Pro Quo	Attackers call numerous **random numbers** within a company, claiming to be from technical support They offer their service to end users in exchange for confidential data or login credentials
Elicitation	Attackers extract information from the victim by engaging him/her in normal and **disarming conversations** Based on the victim's interests, attackers must work to target their elicitation approach to extract the relevant information

Human-based Social Engineering

Impersonation

Impersonation is a common human-based social engineering technique where an attacker pretends to be a legitimate or authorized person. Attackers perform impersonation attacks personally or use a phone or another communication medium to mislead their target and trick them into revealing information. The attacker might impersonate a courier or delivery person, janitor, businessman, client, technician, or they may pretend to be a visitor. Using this technique, the attacker gathers sensitive information by scanning terminals for passwords, searching for important documents on employees' desks, rummaging through bins, and through other tactics. The attacker may even try to overhear confidential conversations and "**shoulder surf**" to obtain sensitive information.

Types of impersonation used in social engineering:

- Posing as a legitimate end-user
- Posing as an important user
- Posing as a technical support agent
- Posing as an internal employee, client, or vendor
- Posing as a repairman
- Abusing the over-helpfulness of the help desk
- Posing as someone with third-party authorization
- Posing as a tech support agent through vishing
- Posing as a trusted authority

Some impersonation tricks that an attacker performs to gather sensitive information about the target organization exploit the human nature of trust, fear, and moral obligation.

- **Posing as a Legitimate End User**

  An attacker might impersonate an employee and then resort to deviant methods to gain access to privileged data. They may provide a false identity to obtain sensitive information.

  Another example is when a "**friend**" of an employee asks them to retrieve information that a bedridden employee supposedly needs. There is a well-recognized rule in social interaction that a favor begets a favor, even if the original "**favor**" is offered without a request from the recipient. This is known as reciprocation. Corporate environments deal with reciprocation daily. Social engineers try to take advantage of this social trait via impersonation.

  Example:

  "Hi! This is John from the finance department. I have forgotten my password. Can I get it?"

- **Posing as an Important User**

  Another behavioral factor that aids a social engineer is people's habit of not questioning authority. People often go out of their way for those whom they perceive to have authority. An attacker posing as an important individual — such as a vice president or director — can often manipulate an unprepared employee. Attackers who take impersonation to a higher level by assuming the identity of an important employee add an element of intimidation. The reciprocation factor also plays a role in this scenario where lower-level employees might go out of their way to help a higher-authority. For example, it is less likely that a help-desk employee will turn down a request from a vice president who is hard-pressed for time and needs some vital information for a meeting. In case an employee refuses to divulge information, social engineers may use authority to intimidate employees and may even threaten to report the employee's misconduct to their supervisors. This technique assumes greater significance when the attacker considers it a challenge to get away with impersonating an authority figure.

  Example:

  "Hi! This is Kevin, the CFO's Secretary. I'm working on an urgent project, and I forgot my system password. Can you help me out?"

- **Posing as a Technical Support Agent**

  Another technique involves an attacker masquerading as a technical support agent, particularly when the victim is not proficient in technical areas. The attacker may pretend to be a hardware vendor, a technician, or a computer supplier. One demonstration at a hacker meeting had the speaker calling Starbucks and asking its employees whether their broadband connection was properly working. The perplexed employee replied that it was the modem that was giving them trouble. The hacker, without giving any credentials, went on to make him read out the credit card number of the last transaction. In a corporate scenario, the attacker may ask employees to reveal their login information, including their password, to fix a nonexistent problem.

Example:

"Sir, this is Mathew, technical support at X Company. Last night we had a system crash here, and we are checking for lost data. Can you give me your ID and password?"

- **Posing as an Internal Employee, Client, or Vendor**

  The attacker usually dresses up in business clothes or another suitable uniform. They enter an organization's building while pretending to be a contractor, client, service personnel, or another authorized person. Then they roam around unnoticed and look for passwords stuck on terminals, extract critical data from wastepaper bins, papers lying on desks, and perform other information gathering. The attacker may also implement other social engineering techniques such as shoulder surfing (observing users typing login credentials or other sensitive information) and eavesdropping (purposely overhearing confidential conversations between employees) to gather sensitive information that might help launch an attack on the organization.

- **Repairman**

  Computer technicians, electricians, and telephone repairpersons are generally unsuspected people. Attackers might impersonate a technician or repair person and enter the organization. They perform normal activities associated with their assumed duty while looking for hidden passwords, critical information on desks, information in trash bins, and other useful information; they sometimes even plant snooping devices in hidden locations.

Impersonation (Vishing)

Vishing (voice or VoIP phishing) is an impersonation technique in which the attacker uses Voice over IP (VoIP) technology to trick individuals into revealing their critical financial and personal information and uses the information for financial gain. The attacker uses caller ID spoofing to forge identification. In many cases, Vishing includes pre-recorded messages and instructions resembling a legitimate financial institution. Through Vishing, the attacker tricks the victim into providing bank account or credit card details for identity verification over the phone.

The attacker may send a fake SMS or email message to the victim, asking the victim to call the financial institution for credit card or bank account verification. In some cases, the victim receives a voice call from the attacker. When the victim calls the number listed in the message or receives the attacker's call, they hear recorded instructions that insist they provide personal and financial information like name, date of birth, social security number, bank account numbers, credit card numbers, or credentials like usernames, passwords. Once the victim provides the information, the recorded message confirms verification of the victim's account.

Discussed below are some tricks attackers use when Vishing to gather sensitive information.

- **Abusing the Over-Helpfulness of Help Desk**

  Help desks are frequently targeted for social engineering attacks for a reason. The staff members are trained to be helpful, and they often give away sensitive information such as passwords and network information without verifying the authenticity of the caller.

  The attacker should know employees' names and have details about the person he is trying to impersonate to be effective. The attacker may call a company's help desk pretending to be a senior official to try to extract sensitive information out of the help desk.

  Example:

  A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

  The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker entrance into the corporate network.

- **Third-party Authorization**

  Another popular technique used by an attacker is to represent themself as an agent authorized by some senior authority in an organization to obtain information on their behalf.

  For instance, when an attacker knows the name of the employee in the target organization authorized to access the required information, they keep a vigil on them so that they can access the required data in the absence of the concerned employee. In this case, the attacker can approach the help desk or other personnel in the company claiming that the employee (authority figure) has requested the information.

  Even though there might be suspicion attached to the authenticity of the request, people tend to overlook this in favor of being helpful in the workplace. People tend to believe that others are being honest when they reference an important person and provide the required information.

  This technique is effective, particularly when the authority figure is on vacation or traveling, making instant verification impossible.

  Example:

  "Hi, I am John, I spoke with Mr. XYZ last week before he went on vacation and he said that you would be able to provide me with the information in his absence. Could you help me out?"

- **Tech Support**

  Like the impersonation of a tech support agent above, an attacker can use vishing to pretend to be a technical support staff member of the target organization's software vendor or contractor to obtain sensitive information. The attacker may pretend to troubleshoot a network problem and ask for the user ID and password of a computer to detect the problem. Believing them to be a troubleshooter, the user would provide the required information.

Example:

Attacker: "Hi, this is Mike from tech support. Some folks in your office have reported a slowdown in logging. Is this true?"

Employee: "Yes, it has seemed slow lately."

Attacker: "Well, we have moved you to a new server, and your service should be much better now. If you want to give me your password, I can check your service. Things will be better from now on."

- **Trusted Authority Figure**

  The most effective method of social engineering is posing as a trusted authority figure. An attacker might pretend to be a fire marshal, superintendent, auditor, director, or other important figure over the phone or in-person to obtain sensitive information from the target.

  Example:

  1. "Hi, I am John Brown. I'm with the external auditor, Arthur Sanderson. We've been requested by the corporate to do a surprise inspection of your disaster recovery procedures. Your department has 10 minutes to show me how you would recover from a website crash."
  2. "Hi, I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car, and I've been trying to get them to outsource their security training needs to us for months.

     They're located just a few miles away, and I think that if I can give them a quick tour of our facilities, it would be enough to push them over the edge and get them to sign up.

     Oh yeah, they are particularly interested in what security precautions we've adopted. It seems someone hacked into their website a while back, which is one of the reasons they're considering our company."
  3. "Hi, I'm with Aircon Express Services. We received a call that the computer room is getting too warm, so I need to check your HVAC system." Using professional-sounding terms like HVAC (Heating, Ventilation, and Air Conditioning) may add just enough credibility to an intruder's masquerade to allow them to access the targeted secured resource.

Eavesdropping

Eavesdropping refers to an unauthorized person listening to a conversation or reading others' messages. It includes the interception of any form of communication, including audio, video, or written, using channels such as telephone lines, email, and instant messaging. An attacker can obtain sensitive information such as passwords, business plans, phone numbers, and addresses.

Shoulder Surfing

Shoulder surfing is the technique of looking over someone's shoulder as they key information into a device. Attackers use shoulder surfing to find out passwords, personal identification numbers, account numbers, and other information. They sometimes even use binoculars and other optical devices or install small cameras to record the actions performed on the victim's system to obtain login details and other sensitive information.

Dumpster Diving

Dumpster diving is the process of retrieving sensitive personal or organizational information by searching through trash bins. Attackers can extract confidential data such as user IDs, passwords, policy numbers, network diagrams, account numbers, bank statements, salary data, source code, sales forecasts, access codes, phone lists, credit card numbers, calendars, and organizational charts on paper or disk. Attackers can then use this information to perform various malicious activities. Sometimes attackers even use pretexts to support their dumpster diving initiatives, such as impersonating a repair person, technician, cleaner, or other legitimate worker.

Information that attackers can obtain by searching through trash bins includes:

- **Phone lists**: Disclose employees' names and contact numbers.
- **Organizational charts**: Disclose details about the structure of the company, physical infrastructure, server rooms, restricted areas, and other organizational data.
- **Email printouts, notes, faxes, and memos**: Reveal personal details of an employee, passwords, contacts, inside working operations, certain useful instructions, and other data.
- **Policy manuals**: Reveal information regarding employment, system use, and operations.
- **Event notes, calendars, or computer use logs**: Reveal information regarding the user's log on and off timings, which helps the attacker to decide on the best time to plan their attack.

Reverse Social Engineering

Generally, reverse social engineering is difficult to carry out. This is primarily because its execution needs a lot of preparation and skills. In reverse social engineering, a perpetrator assumes the role of a knowledgeable professional so that the organization's employees ask them for information. The attacker usually manipulates questions to draw out the required information.

First, the social engineer will cause an incident, creating a problem, and then present themself as the problem solver through general conversation, encouraging employees to ask questions. For example, an employee may ask how this problem has affected files, servers, or equipment. This provides pertinent information to the social engineer. Many different skills and experiences are required to carry out this tactic successfully. Provided below are some of the techniques involved in reverse social engineering:

- **Sabotage**: Once the attacker gains access, they will corrupt the workstation or make it appear corrupted. Under such circumstances, users seek help as they face problems.

- **Marketing**: To ensure that the user calls the attacker, the attacker must advertise. The attacker can do this either by leaving their business card in the target's office or by placing their contact number on the error message itself.
- **Support**: Even if the attacker has already acquired the desired information, they may continue to assist the users so that they remain ignorant of the hacker's identity.

  A good example of a reverse social engineering virus is the "**My Party**" worm. This virus does not rely on sensational subject lines but rather makes use of inoffensive and realistic names for its attachments. By using realistic words, the attacker gains the user's trust, confirms the user's ignorance, and completes the task of information gathering.

Piggybacking

Piggybacking usually implies entry into a building or security area with the consent of the authorized person. For example, an attacker might request an authorized person to unlock a security door, saying that they have forgotten their ID badge. In the interest of common courtesy, the authorized person will allow the attacker to pass through the door.

Tailgating

Tailgating implies accessing a building or secured area without the consent of the authorized person. It is the act of following an authorized person through a secure entrance, as a polite user would open and hold the door for those following them. An attacker, wearing a fake badge, might attempt to enter the secured area by closely following an authorized person through a door that requires key access. They then try to enter the restricted area while pretending to be an authorized person.

Diversion Theft

Diversion theft is a technique where attackers target delivery professionals or transport companies. This technique is also known as "Round the Corner Game" or "Cornet Game." The main objective of this technique is to trick a person responsible for making a genuine delivery into delivering the consignment to the wrong location, thus interrupting the transaction. For example, if the victim is a van driver delivering a package, then that person would be persuaded to drive to a location other than the actual delivery location. Subjecting the van driver to a series of social engineering tricks thus allows the theft to be successful.

Diversion theft can also be practiced by social engineers on the Internet; victims can be persuaded to send sensitive or confidential files to some unassociated person who is not intended to receive them.

Honey Trap

The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

Baiting

Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users. Attackers perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily find them, such as parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company's logo, thereby tricking end-users into trusting it and opening it on their systems. Once the victim connects and opens the device, a malicious file downloads. It infects the system and allows the attacker to take control.

For example, an attacker leaves some bait in the form of a USB drive in the elevator with the label "Employee Salary Information 2019" and a legitimate company's logo. Out of curiosity and greed, the victim picks up the device and opens it up on their system, which downloads the bait. Once the bait is downloaded, a piece of malicious software installs on the victim's system, giving the attacker access.

Quid Pro Quo

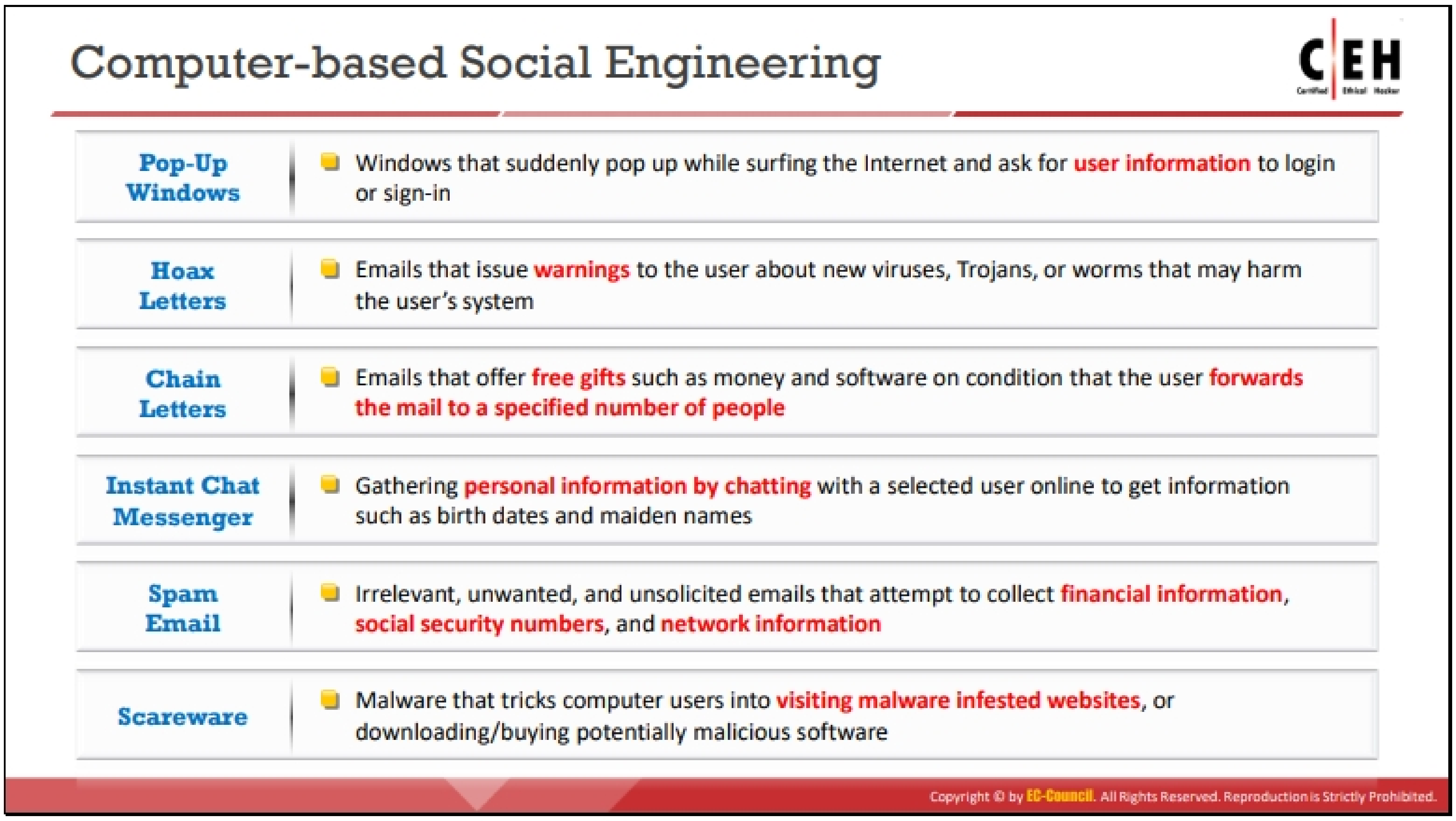
Quid pro quo is a Latin phrase that meaning "something for something." In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials.

For example, an attacker gathers random phone numbers of the employees of a target organization. They then start calling each number, pretending to be from the IT department. The attacker eventually finds someone with a genuine technical issue and offers their service to resolve it. The attacker can then ask the victim to follow a series of steps and to type in the specific commands to install and launch malicious files that contain malware designed to collect sensitive information.

Elicitation

Elicitation is the technique of extracting specific information from the victim by involving them in normal and disarming conversations. In this technique, attackers must possess good social skills to take advantage of professional or social opportunities to communicate with persons who have access to sensitive information. In social engineering, the purpose of elicitation is to extract relevant information to gain access to the target assets.

For example, if an attacker's objective is to obtain the victim's username and password and the conversation with them only yields things that they like, then the attacker must work more on the elicitation process to extract the relevant information.



Computer-based Social Engineering

Pop-Up Windows	Windows that suddenly pop up while surfing the Internet and ask for **user information** to login or sign-in
Hoax Letters	Emails that issue **warnings** to the user about new viruses, Trojans, or worms that may harm the user's system
Chain Letters	Emails that offer **free gifts** such as money and software on condition that the user **forwards the mail to a specified number of people**
Instant Chat Messenger	Gathering **personal information by chatting** with a selected user online to get information such as birth dates and maiden names
Spam Email	Irrelevant, unwanted, and unsolicited emails that attempt to collect **financial information**, **social security numbers**, and **network information**
Scareware	Malware that tricks computer users into **visiting malware infested websites**, or downloading/buying potentially malicious software

Computer-based Social Engineering

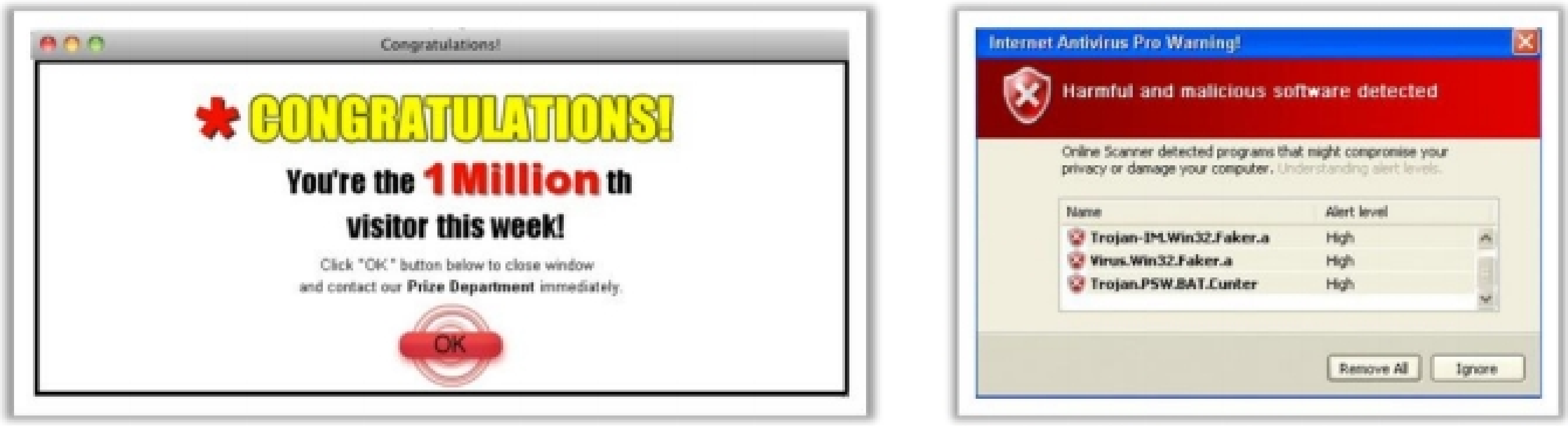
Attackers perform computer-based social engineering using various malicious programs such as viruses, trojans, and spyware, and software applications such as email and instant messaging. Discussed below are types of computer-based social engineering attacks:

- **Pop-Up Windows**

  Pop-ups trick or compel users into clicking a hyperlink that redirects them to fake web pages asking for personal information or downloading malicious programs such as keyloggers, trojans, or spyware.

  The common method of enticing a user to click a button in a pop-up window is by warning of a problem, such as displaying a realistic operating system or application error message, or by offering additional services. A window appears on the screen requesting the user to re-login or warning about an interruption in the host connection, and that the network connection needs re-authentication. When the user follows these instructions, a malicious program installs, extracts the target's sensitive information, and sends it to the attacker's email address or a remote site. This type of attack uses trojans and viruses.

Examples of pop-ups used for tricking users:



*** CONGRATULATIONS!**

You're the 1 Million th visitor this week!

Click "OK" button below to close window and contact our **Prize Department** immediately.

Harmful and malicious software detected

Online Scanner detected programs that might compromise your privacy or damage your computer. Understanding alert levels.

Name	Alert level
Trojan-IM.Win32.Faker.a	High
Virus.Win32.Faker.a	High
Trojan.PSW.BAT.Cunter	High

Figure 9.1: Screenshots showing sample pop-up windows

- **Hoax Letters**

  A hoax is a message warning its recipients of a non-existent computer virus threat. It relies on social engineering to spread its reach. Usually, hoaxes do not cause any physical damage or loss of information; but they cause a loss of productivity and use an organization’s valuable network resources.

- **Chain Letters**

  A chain letter is a message offering free gifts, such as money and software, on the condition that the user forwards the email to a predetermined number of recipients. Common approaches used in chain letters are emotionally convincing stories, “**get-rich-quick**” pyramid schemes, spiritual beliefs, and superstitious threats of bad luck to the recipient if they “break the chain" and fail to pass on the message or simply refuse to read its content. Chain letters also rely on social engineering to spread.

- **Instant Chat Messenger**

  An attacker chats with selected online users via instant chat messengers and tries to gather their personal information such as date of birth or maiden name. They then use the acquired information to crack users’ accounts.

- **Spam Email**

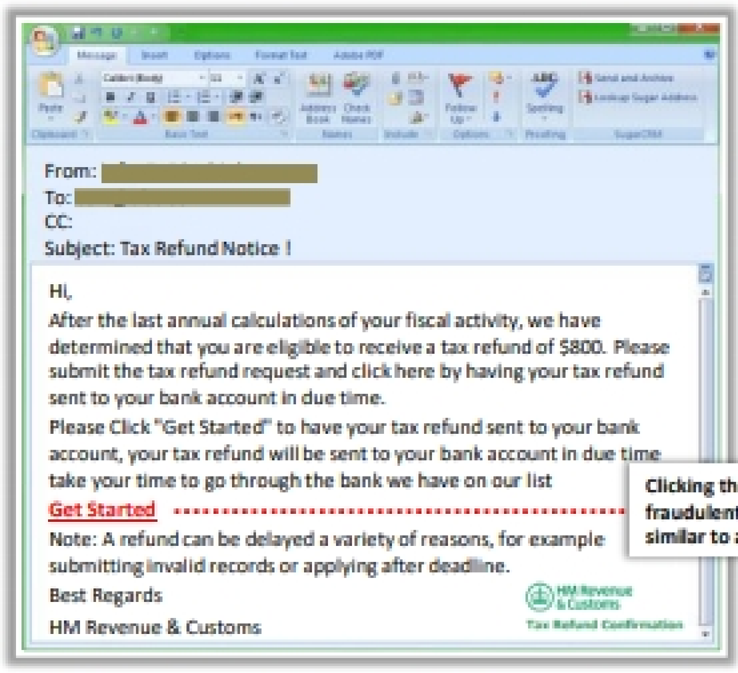
  Spam is irrelevant, unwanted, and unsolicited emails designed to collect financial information such as social security numbers, and network information. Attackers send spam messages to the target to collect sensitive information, such as bank details. Attackers may also send email attachments with hidden malicious programs such as viruses and trojans. Social engineers try to hide the file extension by giving the attachment a long filename.

- **Scareware**

  Scareware is a type of malware that tricks computer users into visiting malware-infested websites or downloading or buying potentially malicious software. Scareware is often seen in pop-ups that tell the target user that their machine has been infected with malware. These pop-ups convincingly appear as though they are coming from a legitimate source such as an antivirus company. Further, these pop-up ads always have a sense of urgency and tell the victim to quickly download the software if they want to get rid of the supposed virus.

Computer-based Social Engineering: Phishing

- Phishing is the practice of **sending an illegitimate email** claiming to be from a **legitimate site** in an attempt to **acquire a user's personal or account information**
- Phishing emails or pop-ups **redirect users to fake webpages** that mimic trustworthy sites, which ask them to submit their personal information

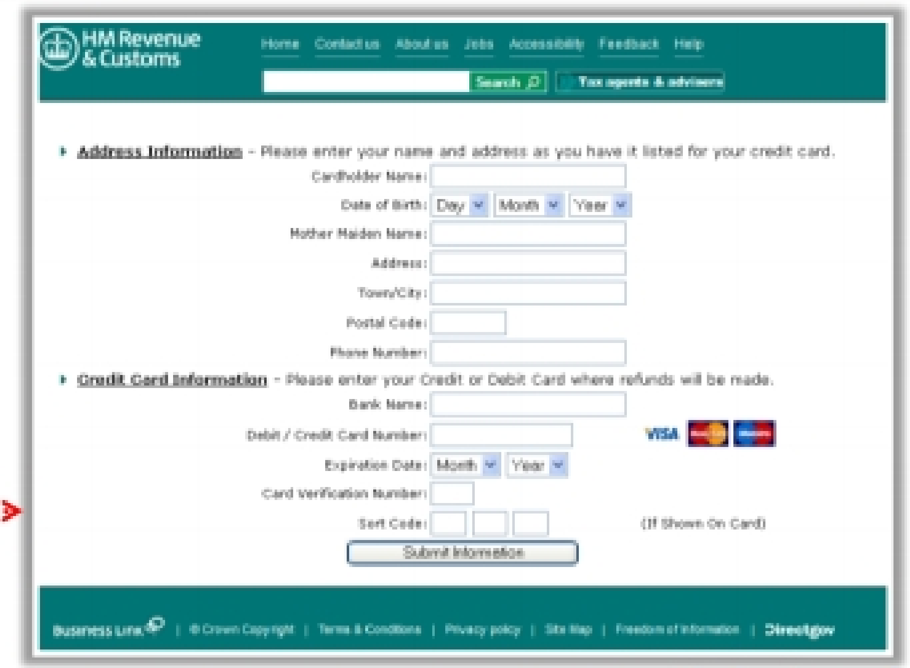

Message
Insert
Options
Format Text
Adobe PDF
Paste
Address Book
Check Names
Follow Up
Spelling
Send and Archive
Lookup Sugar Address
Clipboard
Basic Text
Names
Include
Options
Proofing
SugarCRM

From: [redacted]
To: [redacted]
CC:
Subject: Tax Refund Notice !

Hi,
After the last annual calculations of your fiscal activity, we have determined that you are eligible to receive a tax refund of $800. Please submit the tax refund request and click here by having your tax refund sent to your bank account in due time.
Please Click "Get Started" to have your tax refund sent to your bank account, your tax refund will be sent to your bank account in due time take your time to go through the bank we have on our list
Get Started
Note: A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.
Best Regards
HM Revenue & Customs

HM Revenue & Customs
Tax Refund Confirmation

Clicking the link directs you to a fraudulent web page that looks similar to a genuine HMRC page


HM Revenue & Customs
Home
Contact us
About us
Jobs
Accessibility
Feedback
Help
Search
Tax agents & advisers
VISA
Submit Information
Business Link
© Crown Copyright
Terms & Conditions
Privacy policy
Site Map
Freedom of Information
Directgov

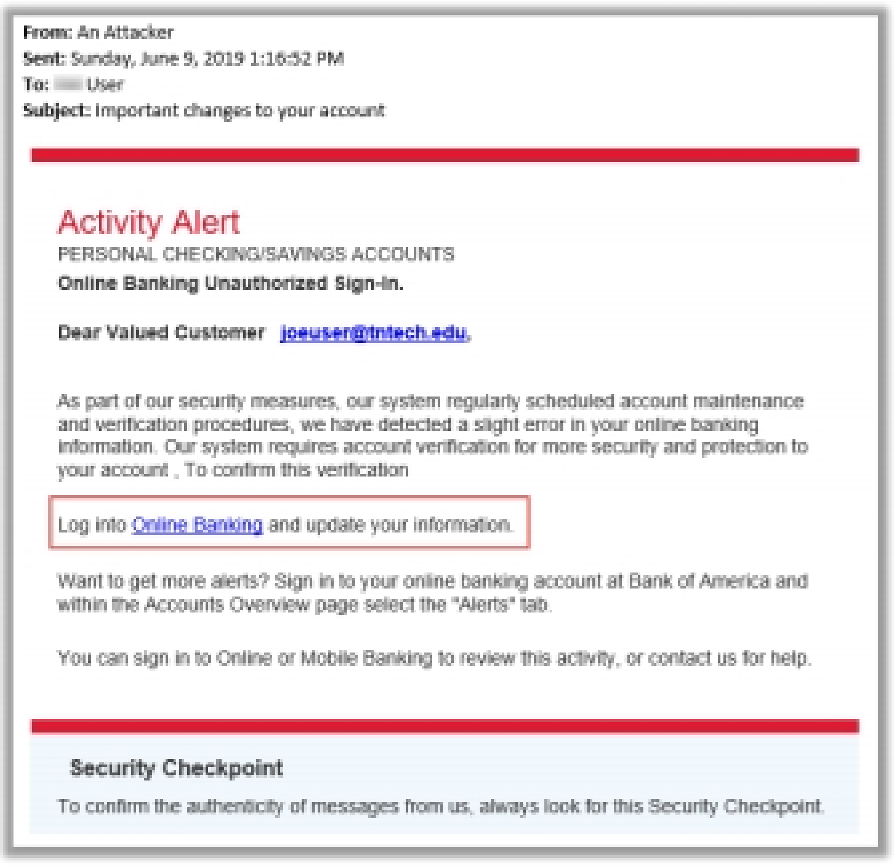
Address Information - Please enter your name and address as you have it listed for your credit card.
Cardholder Name:
Date of Birth: Day Month Year
Mother Maiden Name:
Address:
Town/City:
Postal Code:
Phone Number:

Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.
Bank Name:
Debit / Credit Card Number:
Expiration Date: Month Year
Card Verification Number:
Sort Code: (If Shown On Card)

http://www.hmrc.gov.uk

Computer-based Social Engineering: Phishing (Cont'd)

Examples of Phishing Emails



From: An Attacker
Sent: Sunday, June 9, 2019 1:16:52 PM
To: [redacted] User
Subject: Important changes to your account

Activity Alert
PERSONAL CHECKING/SAVINGS ACCOUNTS
Online Banking Unauthorized Sign-In.

Dear Valued Customer joeuser@tntech.edu,

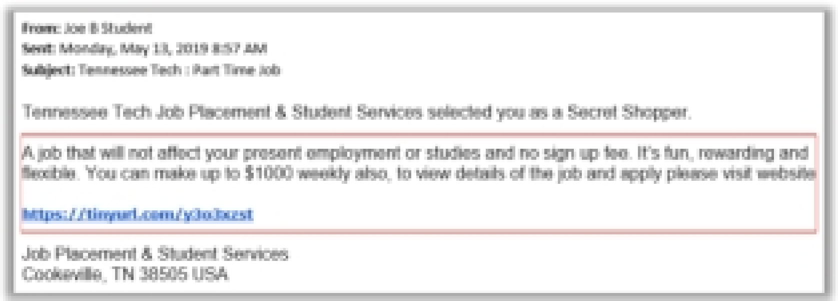
As part of our security measures, our system regularly scheduled account maintenance and verification procedures, we have detected a slight error in your online banking information. Our system requires account verification for more security and protection to your account , To confirm this verification

Log into Online Banking and update your information.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

You can sign in to Online or Mobile Banking to review this activity, or contact us for help.

Security Checkpoint
To confirm the authenticity of messages from us, always look for this Security Checkpoint.



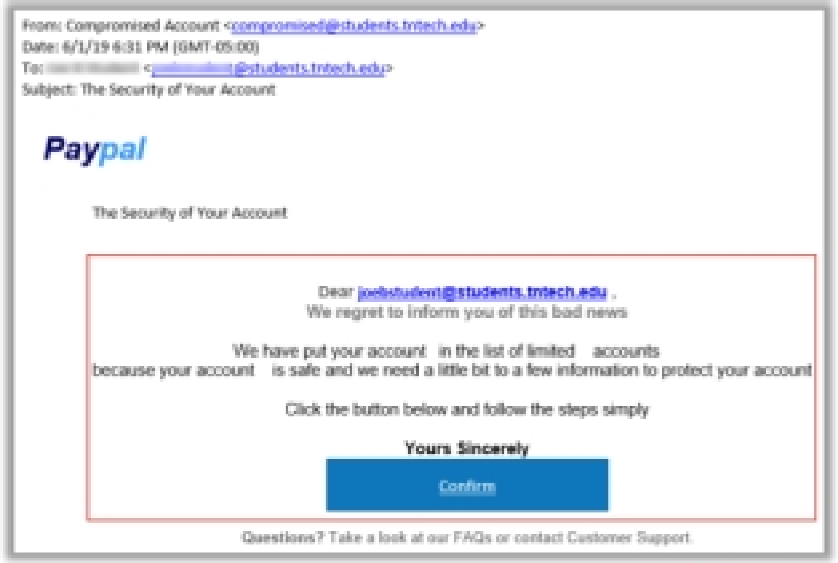
From: Joe B Student
Sent: Monday, May 13, 2019 8:57 AM
Subject: Tennessee Tech : Part Time Job

Tennessee Tech Job Placement & Student Services selected you as a Secret Shopper.

A job that will not affect your present employment or studies and no sign up fee. It's fun, rewarding and flexible. You can make up to $1000 weekly also, to view details of the job and apply please visit website

https://tinyurl.com/y3o3xzst

Job Placement & Student Services
Cookeville, TN 38505 USA



From: Compromised Account <compromised@students.tntech.edu>
Date: 6/1/19 6:31 PM (GMT-05:00)
To: [redacted] <[redacted]@students.tntech.edu>
Subject: The Security of Your Account

The Security of Your Account

Dear joebstudent@students.tntech.edu ,
We regret to inform you of this bad news

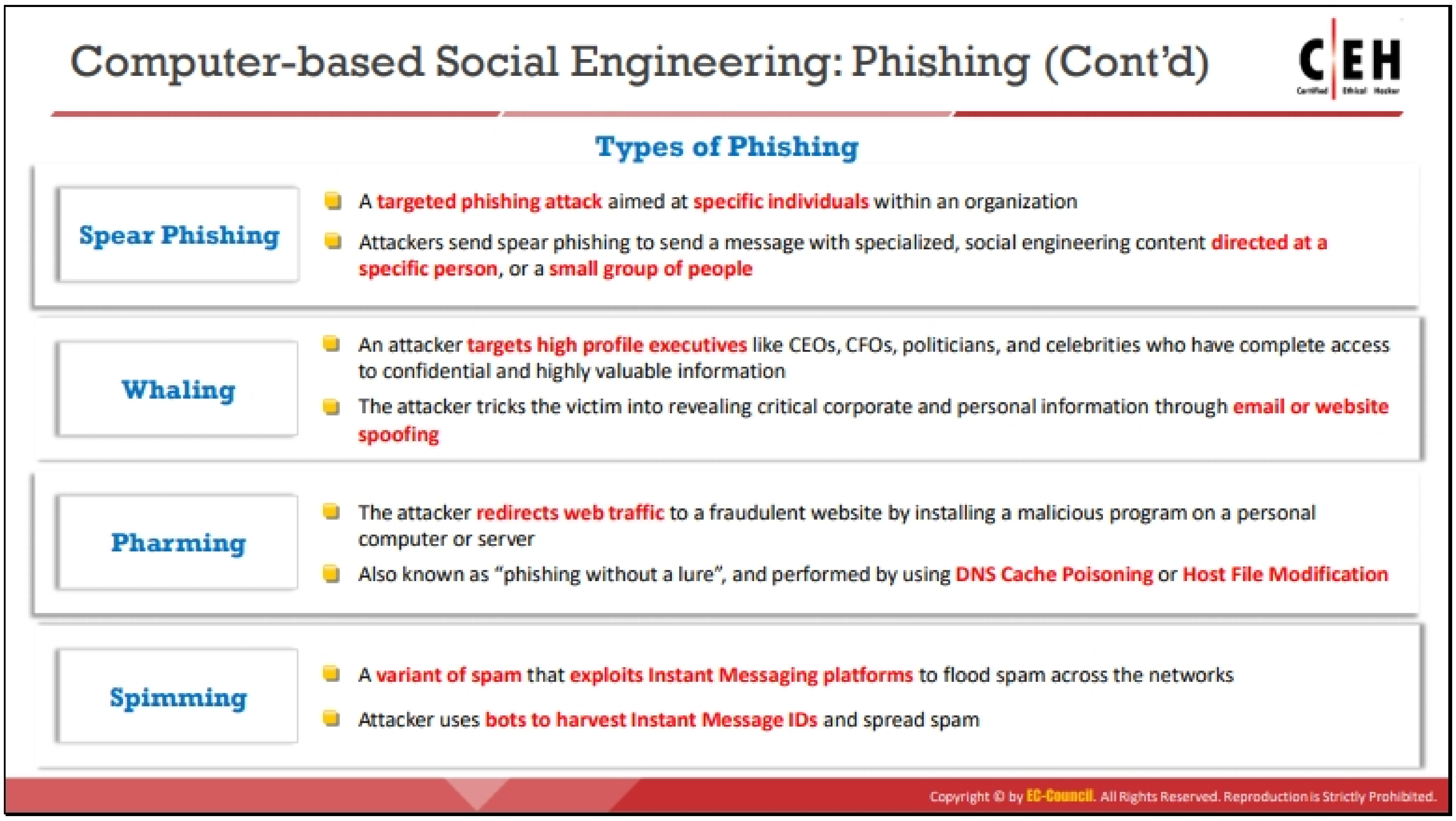
We have put your account in the list of limited accounts
because your account is safe and we need a little bit to a few information to protect your account

Click the button below and follow the steps simply

Yours Sincerely

Questions? Take a look at our FAQs or contact Customer Support.

https://its.tntech.edu



Computer-based Social Engineering: Phishing (Cont'd)

Types of Phishing

Spear Phishing

- A targeted phishing attack aimed at specific individuals within an organization
- Attackers send spear phishing to send a message with specialized, social engineering content directed at a specific person, or a small group of people

Whaling

- An attacker targets high profile executives like CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information
- The attacker tricks the victim into revealing critical corporate and personal information through email or website spoofing

Pharming

- The attacker redirects web traffic to a fraudulent website by installing a malicious program on a personal computer or server
- Also known as "phishing without a lure", and performed by using DNS Cache Poisoning or Host File Modification

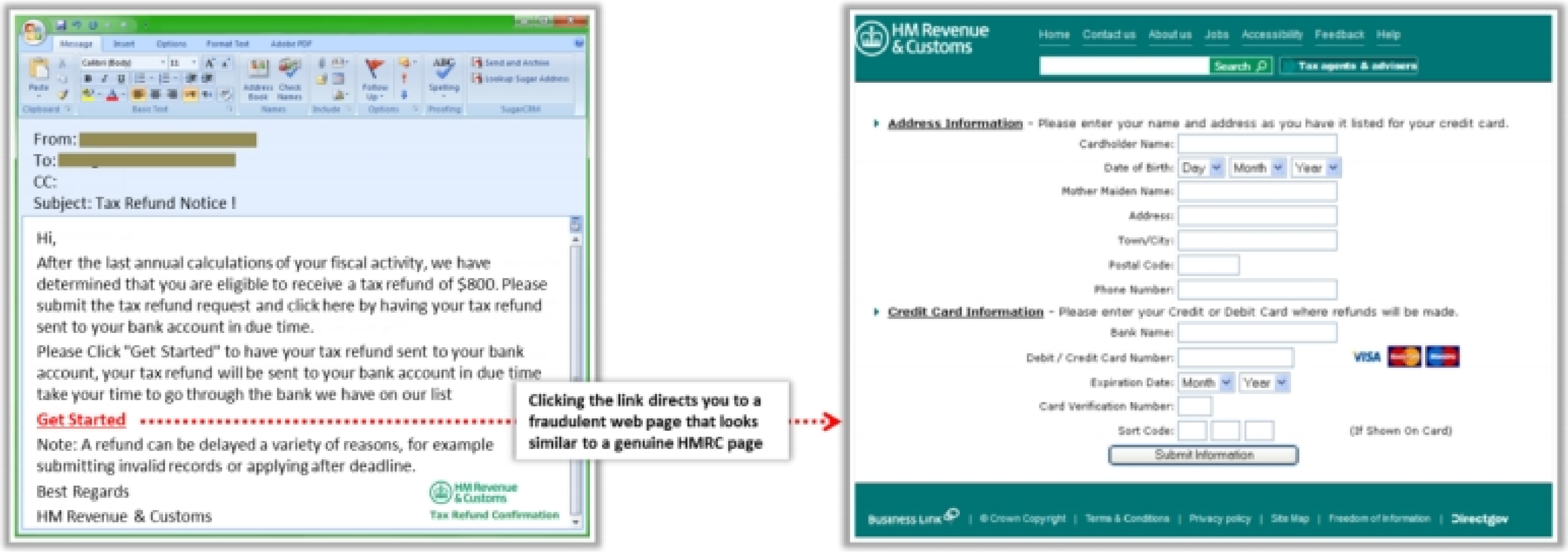
Spimming

- A variant of spam that exploits Instant Messaging platforms to flood spam across the networks
- Attacker uses bots to harvest Instant Message IDs and spread spam

Phishing

Phishing is a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site to acquire a user's personal or account information. The attacker registers a fake domain name, builds a lookalike website, and then mails the fake website's link to users. When a user clicks on the email link, it redirects them to the fake webpage, where they are lured into sharing sensitive details such as their address and credit card information. Some of the reasons behind the success of phishing scams include users' lack of knowledge, being visually deceived, and not paying attention to security indicators.

The screenshot below is an example of an illegitimate email that claims to be from a legitimate sender. The email link redirects users to a fake webpage and asks them to submit their personal or financial details.



From: [redacted]
To: [redacted]
CC:
Subject: Tax Refund Notice !

Hi,

After the last annual calculations of your fiscal activity, we have determined that you are eligible to receive a tax refund of $800. Please submit the tax refund request and click here by having your tax refund sent to your bank account in due time.

Please Click "Get Started" to have your tax refund sent to your bank account, your tax refund will be sent to your bank account in due time take your time to go through the bank we have on our list

Get Started

Note: A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.

Best Regards
HM Revenue & Customs

Clicking the link directs you to a fraudulent web page that looks similar to a genuine HMRC page

Address Information - Please enter your name and address as you have it listed for your credit card.

Cardholder Name:
Date of Birth: Day Month Year
Mother Maiden Name:
Address:
Town/City:
Postal Code:
Phone Number:

Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.

Bank Name:
Debit / Credit Card Number:
Expiration Date: Month Year
Card Verification Number:
Sort Code: (If Shown On Card)

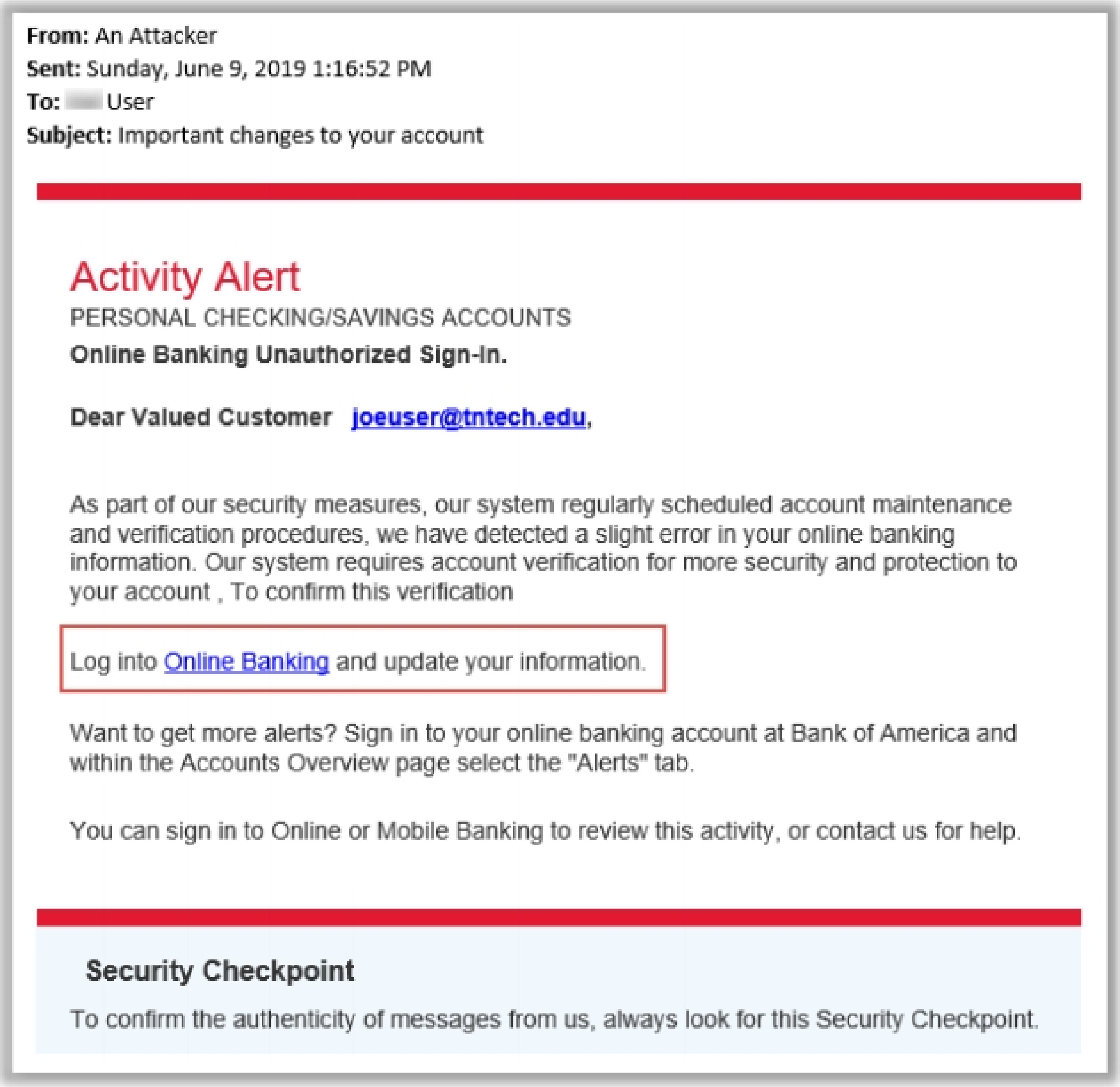
Figure 9.2: Screenshot showing the phishing technique

Examples of Phishing Emails

Source: *https://its.tntech.edu*

Today, most people use internet banking. Many people use Internet banking for all their financial needs, such as online share trading and e-commerce. Phishing involves fraudulently acquiring sensitive information (like passwords and credit card details) by masquerading as a trusted entity.

The target receives an email that appears to be from the bank and requests the user to click on the URL or the link provided. If the user is tricked and provides their username, password, and other information, then the site forwards the information to the attacker, who will use it for nefarious purposes.



From: An Attacker
Sent: Sunday, June 9, 2019 1:16:52 PM
To: [redacted] User
Subject: Important changes to your account

Activity Alert

PERSONAL CHECKING/SAVINGS ACCOUNTS

Online Banking Unauthorized Sign-In.

Dear Valued Customer joeuser@tntech.edu,

As part of our security measures, our system regularly scheduled account maintenance and verification procedures, we have detected a slight error in your online banking information. Our system requires account verification for more security and protection to your account , To confirm this verification

Log into Online Banking and update your information.

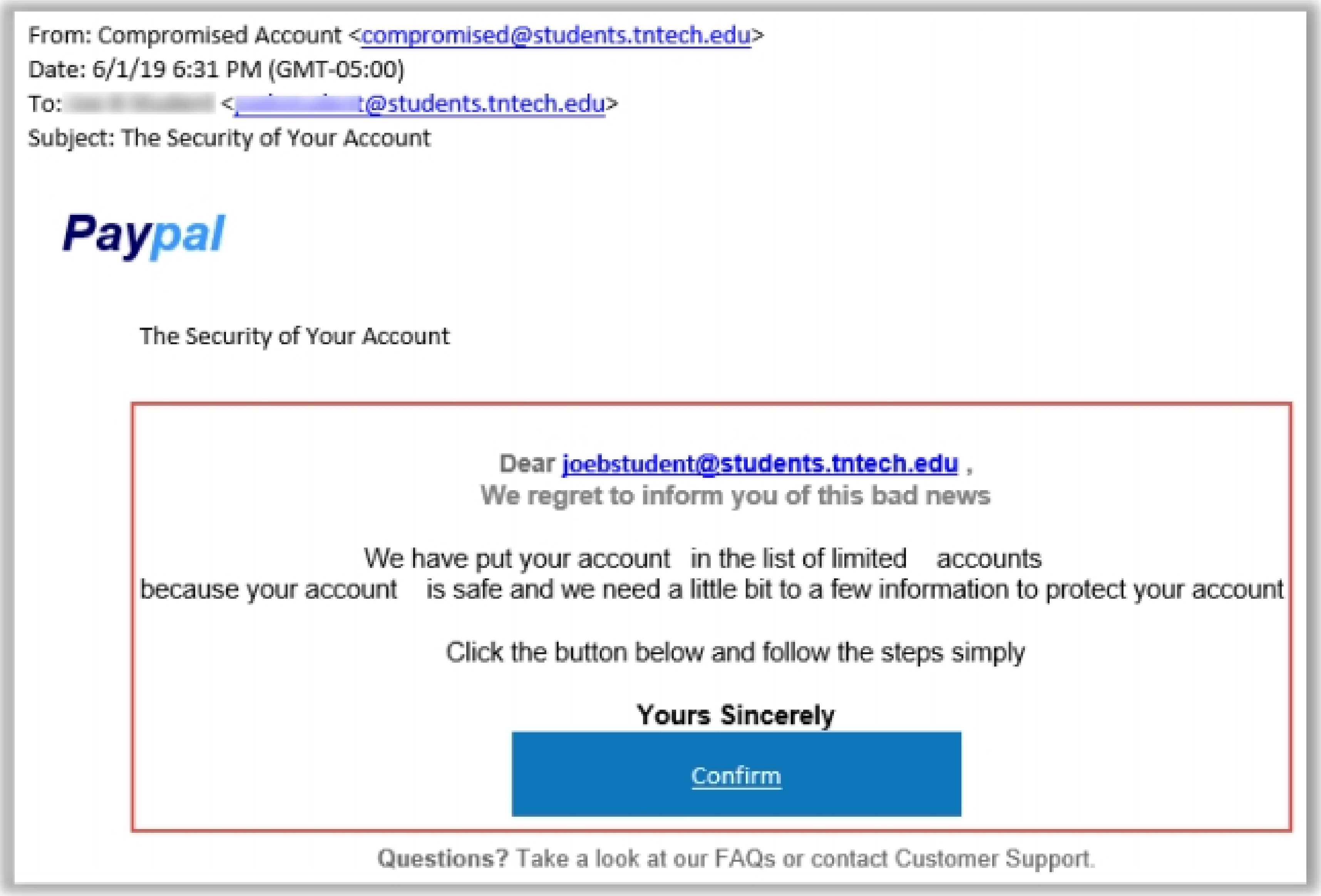
Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

You can sign in to Online or Mobile Banking to review this activity, or contact us for help.

Security Checkpoint

To confirm the authenticity of messages from us, always look for this Security Checkpoint.

Figure 9.3: Screenshot showing a phishing email



From: Compromised Account <compromised@students.tntech.edu>
Date: 6/1/19 6:31 PM (GMT-05:00)
To: [redacted] <[redacted]t@students.tntech.edu>
Subject: The Security of Your Account

Paypal

The Security of Your Account

Dear joebstudent@students.tntech.edu ,
We regret to inform you of this bad news

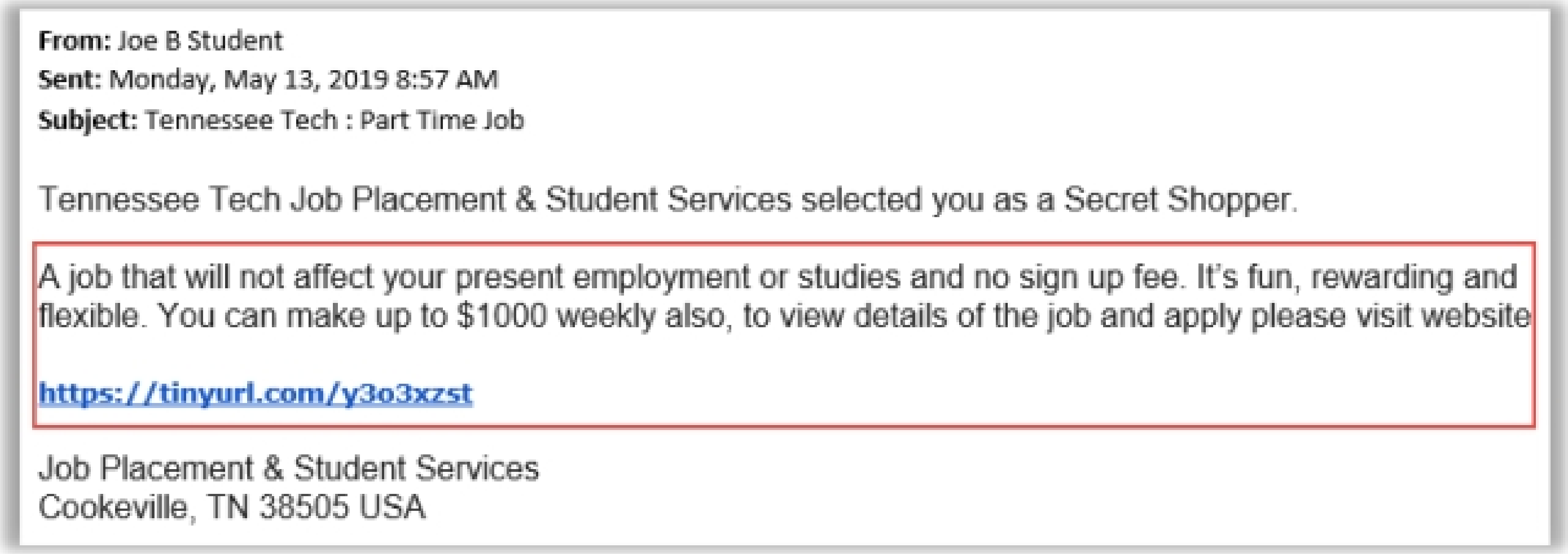
We have put your account in the list of limited accounts
because your account is safe and we need a little bit to a few information to protect your account

Click the button below and follow the steps simply

Yours Sincerely

Questions? Take a look at our FAQs or contact Customer Support.

Figure 9.4: Screenshot showing a phishing email



From: Joe B Student
Sent: Monday, May 13, 2019 8:57 AM
Subject: Tennessee Tech : Part Time Job

Tennessee Tech Job Placement & Student Services selected you as a Secret Shopper.

A job that will not affect your present employment or studies and no sign up fee. It's fun, rewarding and flexible. You can make up to $1000 weekly also, to view details of the job and apply please visit website

https://tinyurl.com/y3o3xzst

Job Placement & Student Services
Cookeville, TN 38505 USA

Figure 9.5: Screenshot showing a phishing email

Types of Phishing

- **Spear Phishing**

  Instead of sending out thousands of emails, some attackers opt for "**spear phishing**" and use specialized social engineering content directed at a specific employee or small group of employees in an organization to steal sensitive data such as financial information and trade secrets.

  Spear phishing messages seem to come from a trusted source with an official-looking website. The email also appears to be from an individual from the recipient's company, generally someone in a position of authority. In reality, the message is sent by an attacker attempting to obtain critical information about a specific recipient and their organization, such as login credentials, credit card details, bank account numbers, passwords, confidential documents, financial information, and trade secrets. Spear phishing generates a higher response rate compared to a normal phishing attack, as it appears to be from a trusted company source.

- **Whaling**

  A whaling attack is a type of phishing that targets high profile executives like CEO, CFO, politicians, and celebrities who have complete access to confidential and highly valuable information. It is a social engineering trick in which the attacker tricks the victim into revealing critical corporate and personal information (like bank account details, employee details, customer information, and credit card details), generally, through email or website spoofing. Whaling is different from a normal phishing attack; the email or website used for the attack is carefully designed, usually targeting someone in the executive leadership.

- **Pharming**

  Pharming is a social engineering technique in which the attacker executes malicious programs on a victim's computer or server, and when the victim enters any URL or domain name, it automatically redirects the victim's traffic to an attacker-controlled website. This attack is also known as "Phishing without a Lure." The attacker steals confidential information like credentials, banking details, and other information related to web-based services.

  Pharming attack can be performed in two ways: DNS Cache Poisoning and Host File Modification

  DNS Cache Poisoning:

  - The attacker performs DNS Cache Poisoning on the targeted DNS server.
  - The attacker modifies the IP address of the target website "www.targetwebsite.com" to that of a fake website "www.hackerwebsite.com."
  - When the victim enters the target website's URL in the browser's address bar, a request is sent to the DNS server to obtain the IP address of the target website.
  - The DNS server returns a fake IP address that is already modified by the attacker.
  - Finally, the victim is redirected to the fake website.

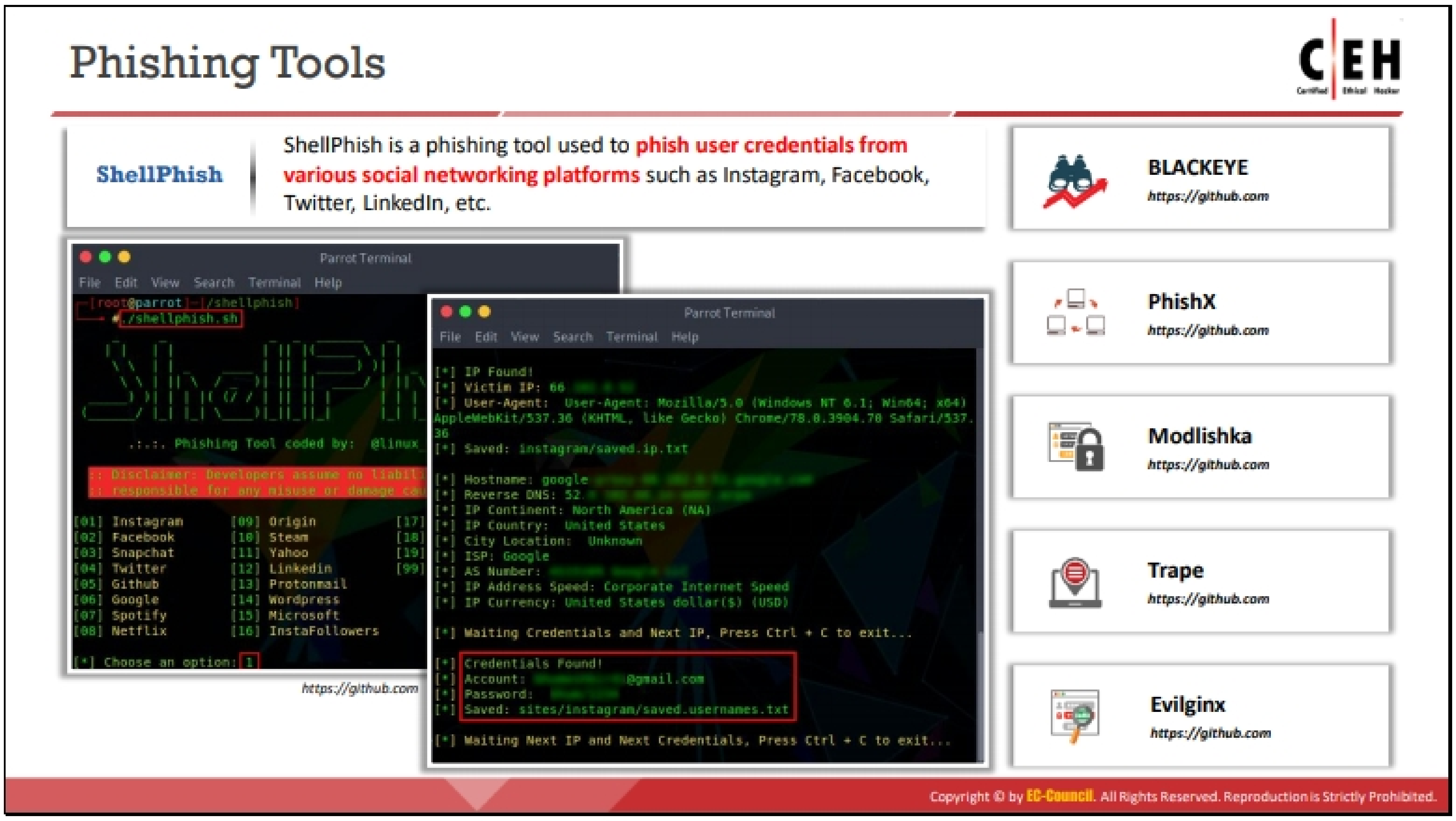
  Host File Modification:

  - An attacker sends a malicious code as an email attachment.
  - When the user clicks on the attachment, the code executes and modifies local host files on the user's computer.
  - When the victim enters the target website's URL in the browsers address bar, the compromised host file automatically redirects the user's traffic to the fraudulent website controlled by the hacker.

  Pharming attacks can also be performed using malware like Trojan horses or worms.

- **Spimming**

  SPIM (Spam over Instant Messaging) exploits Instant Messaging platforms and uses IM as a tool to spread spam. A person who generates spam over IM is called Spimmer. Spimmers generally make use of bots (an application that executes automated tasks over the network) to harvest Instant Message IDs and forward spam messages to them. SPIM messages, like email spam, generally include advertisements and malware as an attachment or embedded hyperlink. The user clicks the attachment and is redirected to a malicious website that collects financial and personal information like credentials, bank account, and credit card details.



Phishing Tools

ShellPhish

ShellPhish is a phishing tool used to **phish user credentials from various social networking platforms** such as Instagram, Facebook, Twitter, LinkedIn, etc.

```
┌─[root@parrot]─[~/shellphish]
└──╼ #./shellphish.sh

      .:.:. Phishing Tool coded by:  @linux_

 :: Disclaimer: Developers assume no liabil
 :: responsible for any misuse or damage cau

[01] Instagram         [09] Origin            [17]
[02] Facebook          [10] Steam             [18]
[03] Snapchat          [11] Yahoo             [19]
[04] Twitter           [12] Linkedin          [99]
[05] Github            [13] Protonmail
[06] Google            [14] Wordpress
[07] Spotify           [15] Microsoft
[08] Netflix           [16] InstaFollowers

[*] Choose an option: 1
```

https://github.com

```
[*] IP Found!
[*] Victim IP: 66 [redacted]
[*] User-Agent:  User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.
36
[*] Saved: instagram/saved.ip.txt

[*] Hostname: google [redacted]
[*] Reverse DNS: 52 [redacted]
[*] IP Continent: North America (NA)
[*] IP Country:  United States
[*] City Location:  Unknown
[*] ISP: Google
[*] AS Number: [redacted]
[*] IP Address Speed: Corporate Internet Speed
[*] IP Currency: United States dollar($) (USD)

[*] Waiting Credentials and Next IP, Press Ctrl + C to exit...

[*] Credentials Found!
[*] Account: [redacted]@gmail.com
[*] Password: [redacted]
[*] Saved: sites/instagram/saved.usernames.txt

[*] Waiting Next IP and Next Credentials, Press Ctrl + C to exit...
```

BLACKEYE
https://github.com

PhishX
https://github.com

Modlishka
https://github.com

Trape
https://github.com

Evilginx
https://github.com

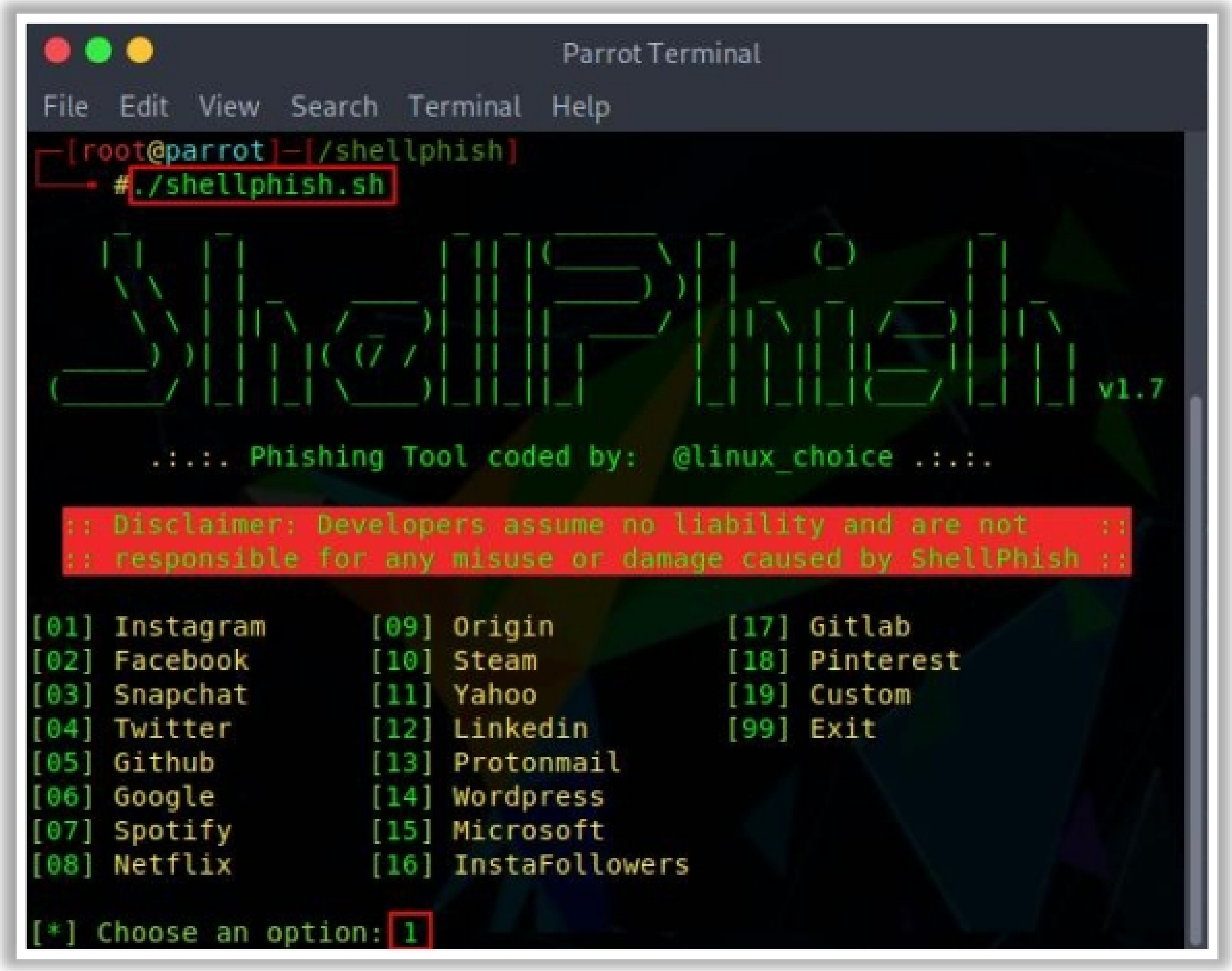
Phishing Tools

Phishing tools can be used by attackers to generate fake login pages to capture usernames and passwords, send spoofed emails, and obtain the victim's IP address and session cookies. This information can further be used by the attacker, who will use it to impersonate a legitimate user and launch further attacks on the target organization.

- **ShellPhish**

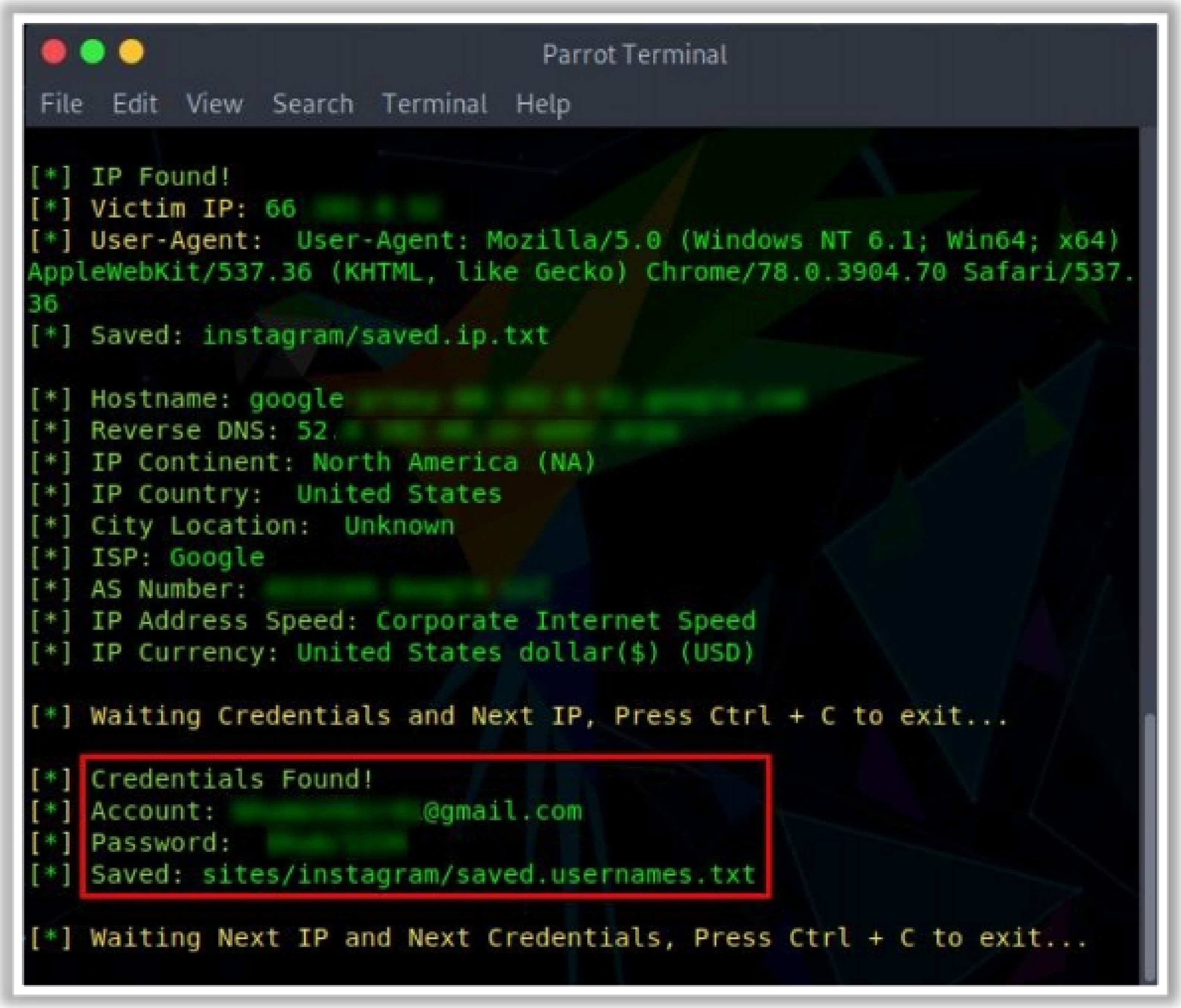
  Source: *https://github.com*

  ShellPhish is a phishing tool used to phish user credentials from various social networking platforms such as Instagram, Facebook, Twitter, and LinkedIn. It also displays the victim system's public IP address, browser information, hostname, geolocation, and other information.



```
┌─[root@parrot]─[/shellphish]
└──╼ #./shellphish.sh

                                                              v1.7

      .:.:. Phishing Tool coded by:  @linux_choice .:.:.

 :: Disclaimer: Developers assume no liability and are not    ::
 :: responsible for any misuse or damage caused by ShellPhish ::

[01] Instagram      [09] Origin          [17] Gitlab
[02] Facebook       [10] Steam           [18] Pinterest
[03] Snapchat       [11] Yahoo           [19] Custom
[04] Twitter        [12] Linkedin        [99] Exit
[05] Github         [13] Protonmail
[06] Google         [14] Wordpress
[07] Spotify        [15] Microsoft
[08] Netflix        [16] InstaFollowers

[*] Choose an option: 1
```

Figure 9.6: Screenshot of ShellPhish

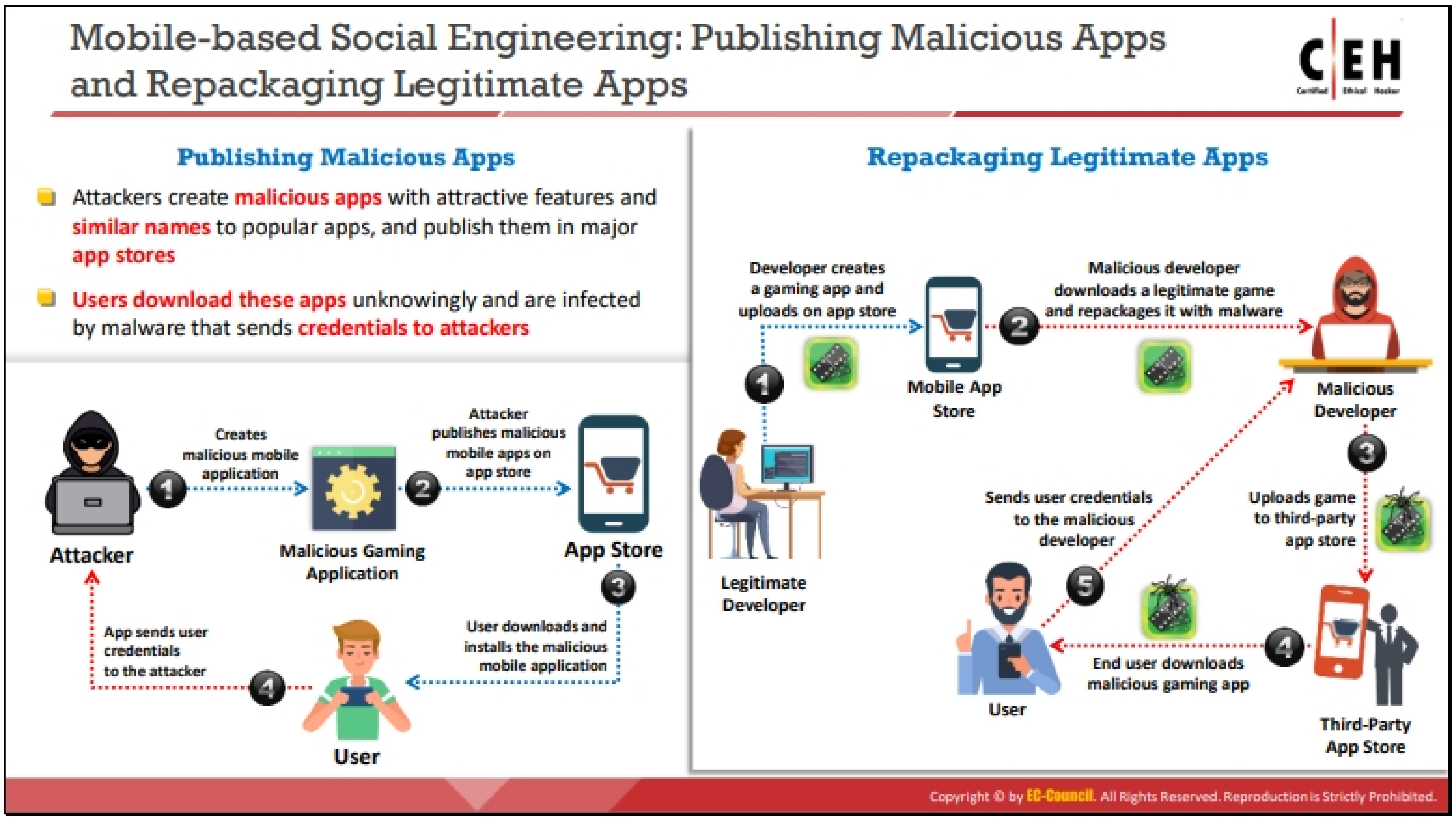


```
[*] IP Found!
[*] Victim IP: 66[redacted]
[*] User-Agent:  User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.
36
[*] Saved: instagram/saved.ip.txt

[*] Hostname: google[redacted]
[*] Reverse DNS: 52[redacted]
[*] IP Continent: North America (NA)
[*] IP Country:  United States
[*] City Location:  Unknown
[*] ISP: Google
[*] AS Number: [redacted]
[*] IP Address Speed: Corporate Internet Speed
[*] IP Currency: United States dollar($) (USD)

[*] Waiting Credentials and Next IP, Press Ctrl + C to exit...

[*] Credentials Found!
[*] Account: [redacted]@gmail.com
[*] Password: [redacted]
[*] Saved: sites/instagram/saved.usernames.txt

[*] Waiting Next IP and Next Credentials, Press Ctrl + C to exit...
```

Figure 9.7: Screenshot showing the output of ShellPhish

Some additional phishing tools are listed below:

- BLACKEYE (*https://github.com*)
- PhishX (*https://github.com*)
- Modlishka (*https://github.com*)
- Trape (*https://github.com*)
- Evilginx (*https://github.com*)



Mobile-based Social Engineering: Publishing Malicious Apps and Repackaging Legitimate Apps

Publishing Malicious Apps

- Attackers create **malicious apps** with attractive features and **similar names** to popular apps, and publish them in major **app stores**
- **Users download these apps** unknowingly and are infected by malware that sends **credentials to attackers**

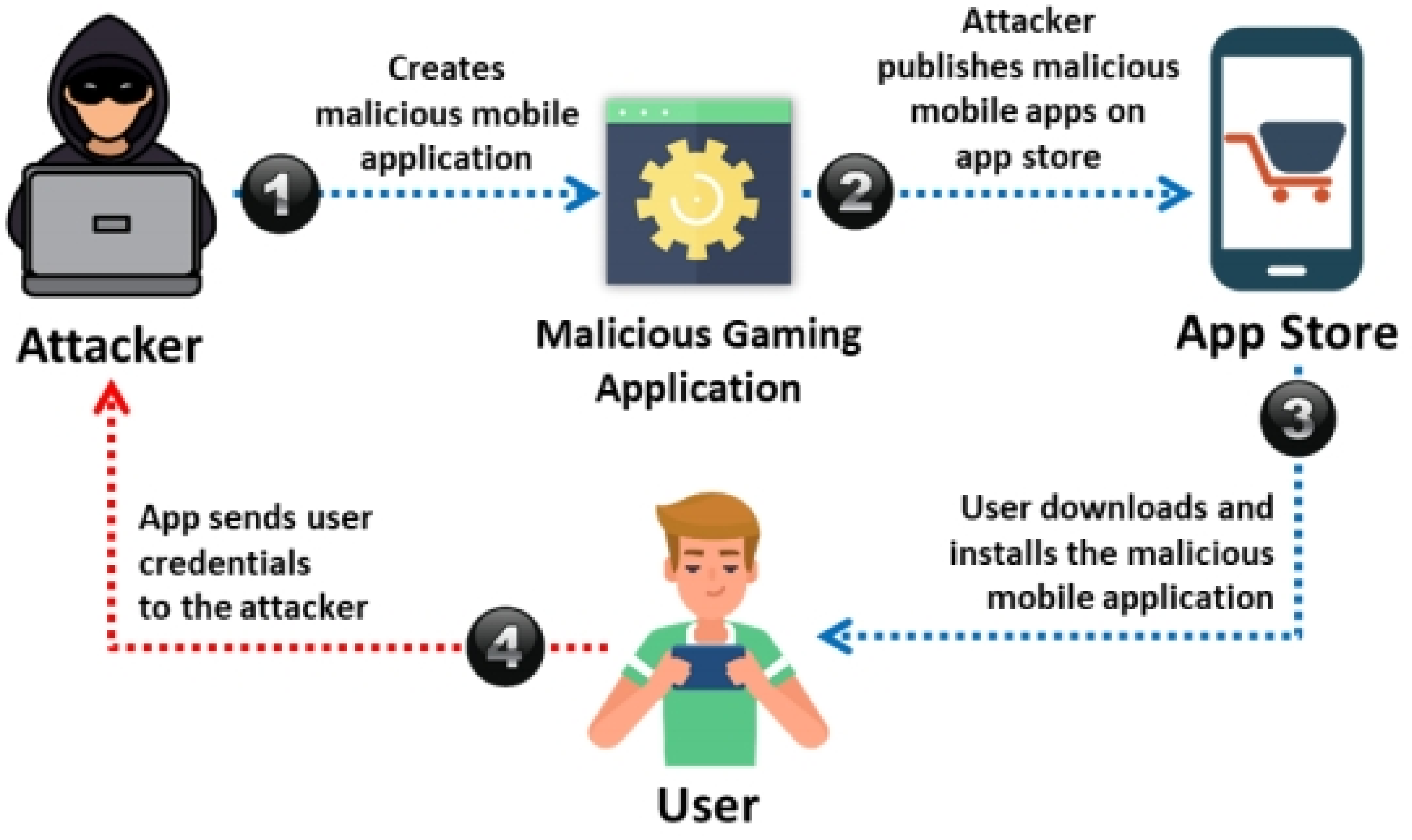
Repackaging Legitimate Apps

C|EH Certified Ethical Hacker
Attacker
1
Creates malicious mobile application
Malicious Gaming Application
2
Attacker publishes malicious mobile apps on app store
App Store
3
User downloads and installs the malicious mobile application
User
4
App sends user credentials to the attacker
Developer creates a gaming app and uploads on app store
1
Legitimate Developer
Mobile App Store
2
Malicious developer downloads a legitimate game and repackages it with malware
Malicious Developer
3
Uploads game to third-party app store
Third-Party App Store
4
End user downloads malicious gaming app
User
5
Sends user credentials to the malicious developer

Mobile-based Social Engineering

Publishing Malicious Apps

In mobile-based social engineering, the attacker performs a social engineering attack using malicious mobile apps. The attacker first creates the malicious application — such as a gaming app with attractive features — and publishes it on major application stores using the popular names. Unaware of the malicious application, a user will download it onto their mobile device, believing it to be genuine. Once the application is installed, the device is infected by malware that sends the user's credentials (usernames, passwords), contact details, and other information to the attacker.



Attacker
1
Creates malicious mobile application
Malicious Gaming Application
2
Attacker publishes malicious mobile apps on app store
App Store
3
User downloads and installs the malicious mobile application
User
4
App sends user credentials to the attacker

Figure 9.8: Publishing malicious apps

Repackaging Legitimate Apps

Sometimes malware can be hidden within legitimate apps. A legitimate developer creates legitimate gaming applications. Platform vendors create centralized marketplaces to allow mobile users to conveniently browse and install these games and apps. Usually, developers submit gaming applications to these marketplaces, making them available to thousands of mobile users. A malicious developer downloads a legitimate game, repackages it with malware, and uploads it to the third-party application store. Once a user downloads the malicious application, the malicious program installed on the user's mobile device collects the user's information and sends it to the attacker.

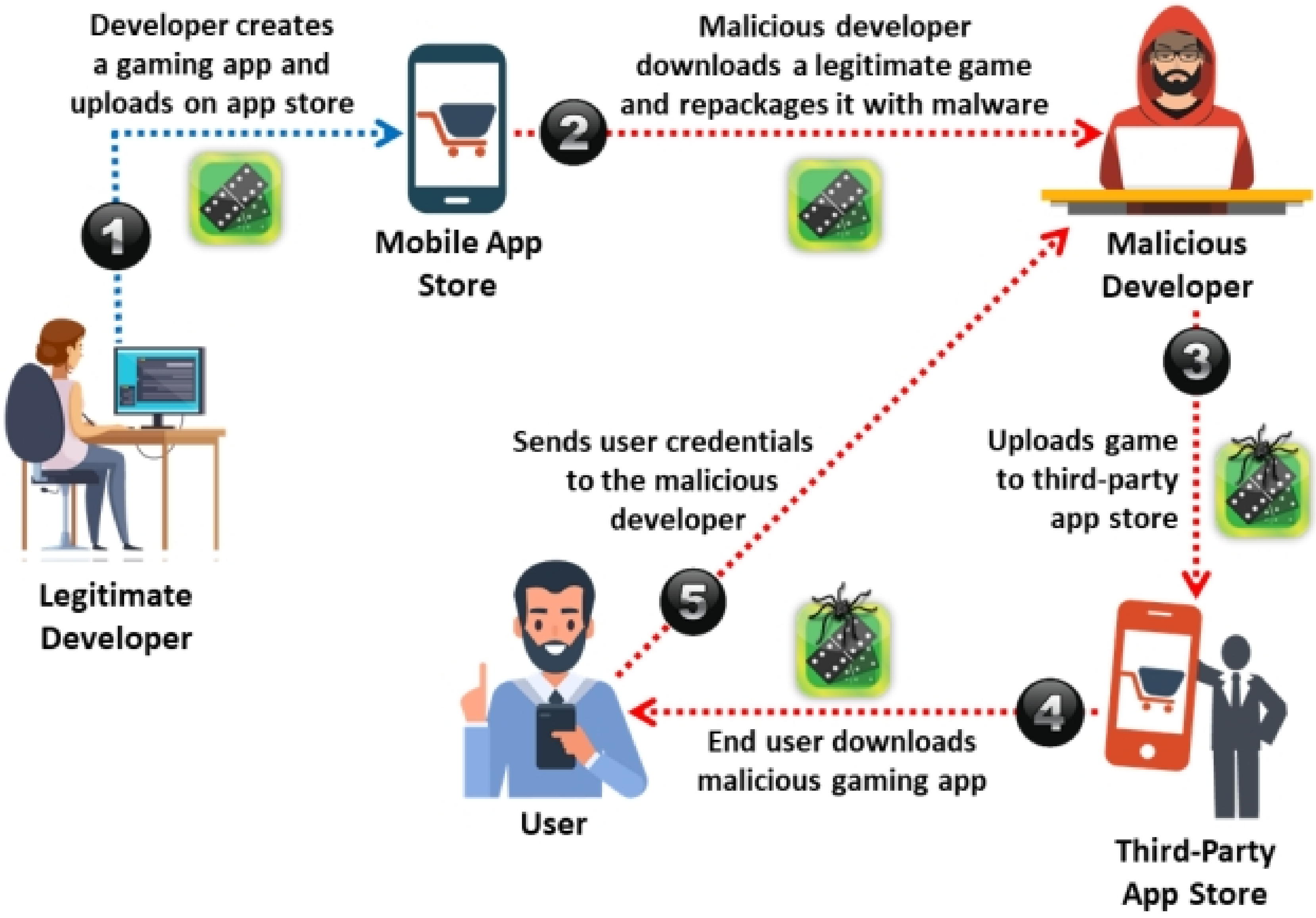
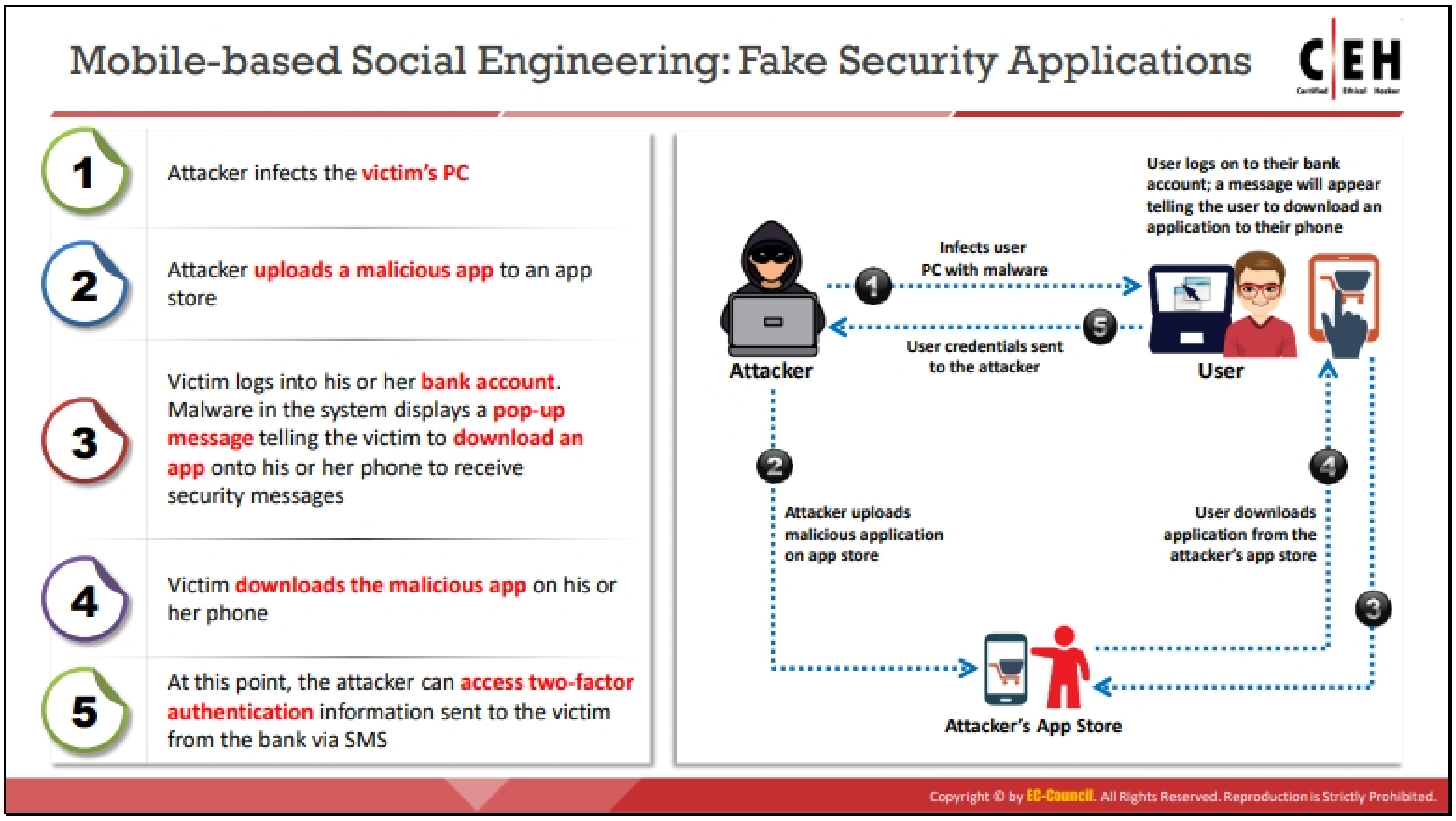

Developer creates a gaming app and uploads on app store
1
Mobile App Store
2
Malicious developer downloads a legitimate game and repackages it with malware
Malicious Developer
3
Legitimate Developer
Sends user credentials to the malicious developer
Uploads game to third-party app store
5
User
4
End user downloads malicious gaming app
Third-Party App Store

Figure 9.9: Repackaging legitimate apps



Mobile-based Social Engineering: Fake Security Applications

1. Attacker infects the **victim's PC**
2. Attacker **uploads a malicious app** to an app store
3. Victim logs into his or her **bank account**. Malware in the system displays a **pop-up message** telling the victim to **download an app** onto his or her phone to receive security messages
4. Victim **downloads the malicious app** on his or her phone
5. At this point, the attacker can **access two-factor authentication** information sent to the victim from the bank via SMS

Attacker
1 Infects user PC with malware
User logs on to their bank account; a message will appear telling the user to download an application to their phone
User
5 User credentials sent to the attacker
2 Attacker uploads malicious application on app store
4 User downloads application from the attacker's app store
3
Attacker's App Store

Fake Security Applications

Attackers may send a fake security application to perform mobile-based social engineering. In this attack, the attacker first infects the victim's computer by sending something malicious. They then upload a malicious application to an app store. When the victim logs on to their bank account, malware in the system displays a pop-up message telling the victim that they need to download an application on their phone to receive a message from security. The victim downloads the application from the attacker's app store, believing they are downloading a genuine app. Once the user downloads the application, the attacker obtains confidential information such as bank account login credentials (username and password), whereupon a second authentication is sent by the bank to the victim via SMS. Using that information, the attacker accesses the victim's bank account.

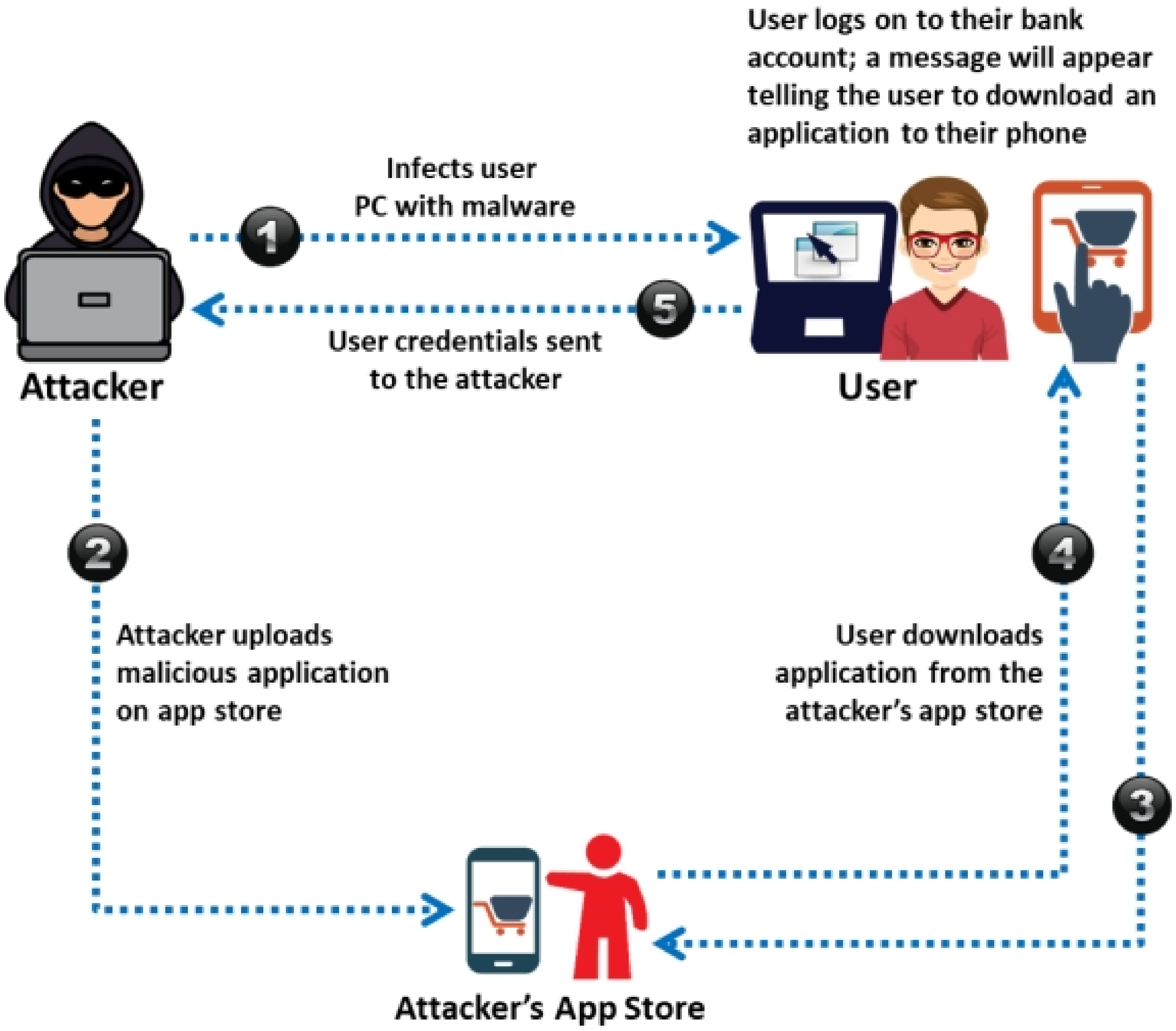
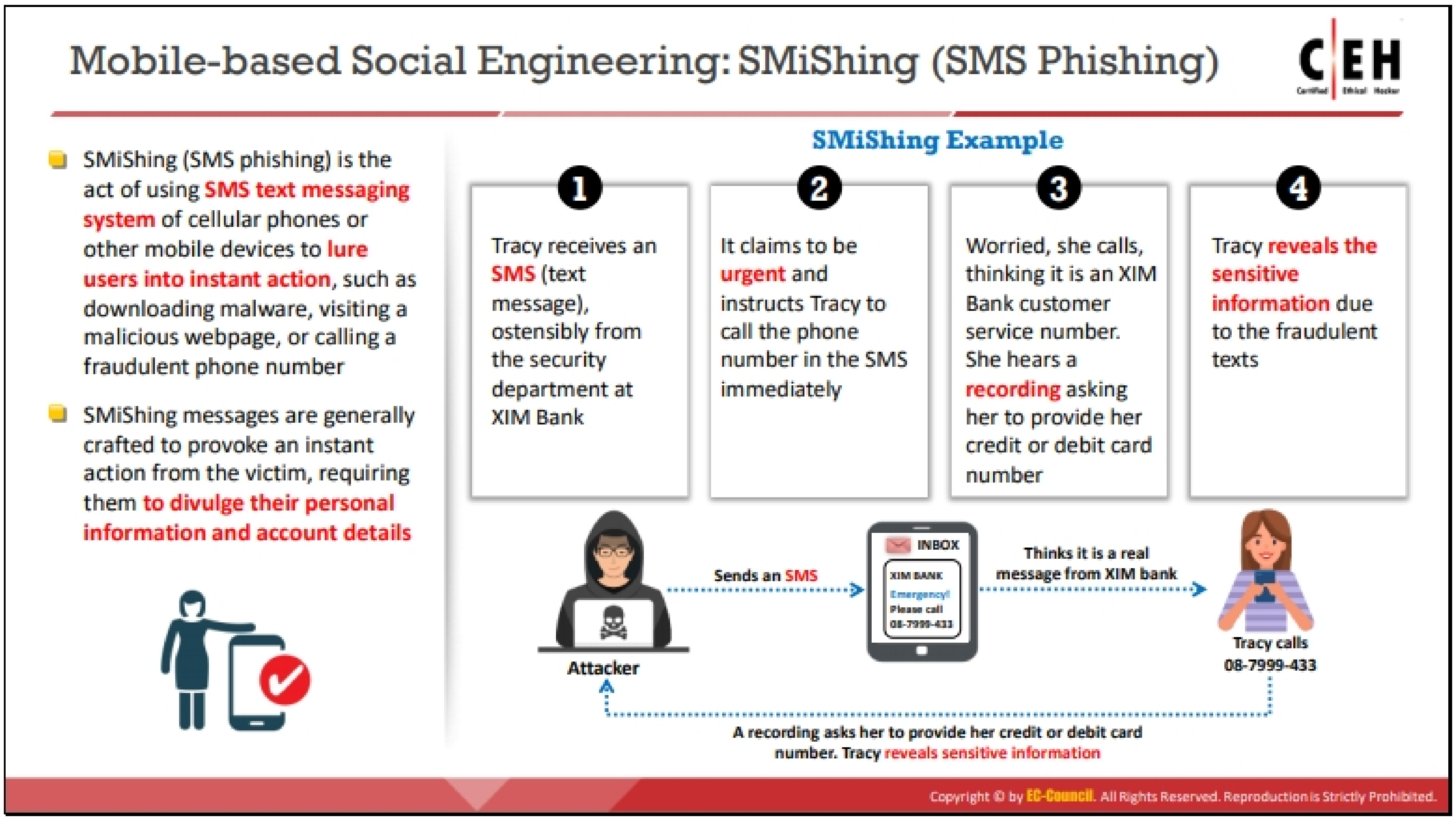

User logs on to their bank account; a message will appear telling the user to download an application to their phone
Infects user PC with malware
1
5
User credentials sent to the attacker
Attacker
User
2
Attacker uploads malicious application on app store
4
User downloads application from the attacker's app store
3
Attacker's App Store

Figure 9.10: Fake security applications



Mobile-based Social Engineering: SMiShing (SMS Phishing)

- SMiShing (SMS phishing) is the act of using **SMS text messaging system** of cellular phones or other mobile devices to **lure users into instant action**, such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number
- SMiShing messages are generally crafted to provoke an instant action from the victim, requiring them **to divulge their personal information and account details**

SMiShing Example

❶ Tracy receives an **SMS** (text message), ostensibly from the security department at XIM Bank

❷ It claims to be **urgent** and instructs Tracy to call the phone number in the SMS immediately

❸ Worried, she calls, thinking it is an XIM Bank customer service number. She hears a **recording** asking her to provide her credit or debit card number

❹ Tracy **reveals the sensitive information** due to the fraudulent texts

Attacker

Sends an SMS

INBOX
XIM BANK
Emergency!
Please call
08-7999-433

Thinks it is a real message from XIM bank

Tracy calls
08-7999-433

A recording asks her to provide her credit or debit card number. Tracy reveals sensitive information

SMiShing (SMS Phishing)

Sending SMS is another technique used by attackers in performing mobile-based social engineering. In SMiShing (SMS Phishing), the SMS text messaging system is used to lure users into taking instant action such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number. SMiShing messages are crafted to provoke an instant action from the victim, requiring them to divulge their personal information and account details.

Consider Tracy, a software engineer working in a reputed company. She receives an SMS ostensibly from the security department of XIM Bank. It claims to be urgent, and the message says that Tracy should call the phone number listed in the SMS immediately. Worried, she calls to check on her account, believing it to be an authentic XIM Bank customer service phone number. A recorded message asks her to provide her credit or debit card number, as well as her password. Tracy believes it is a genuine message and shares sensitive information.

Sometimes a message claims that the user has won money or has been randomly selected as a lucky winner and that they merely need to pay a nominal fee and share their email address, contact number, or other information.

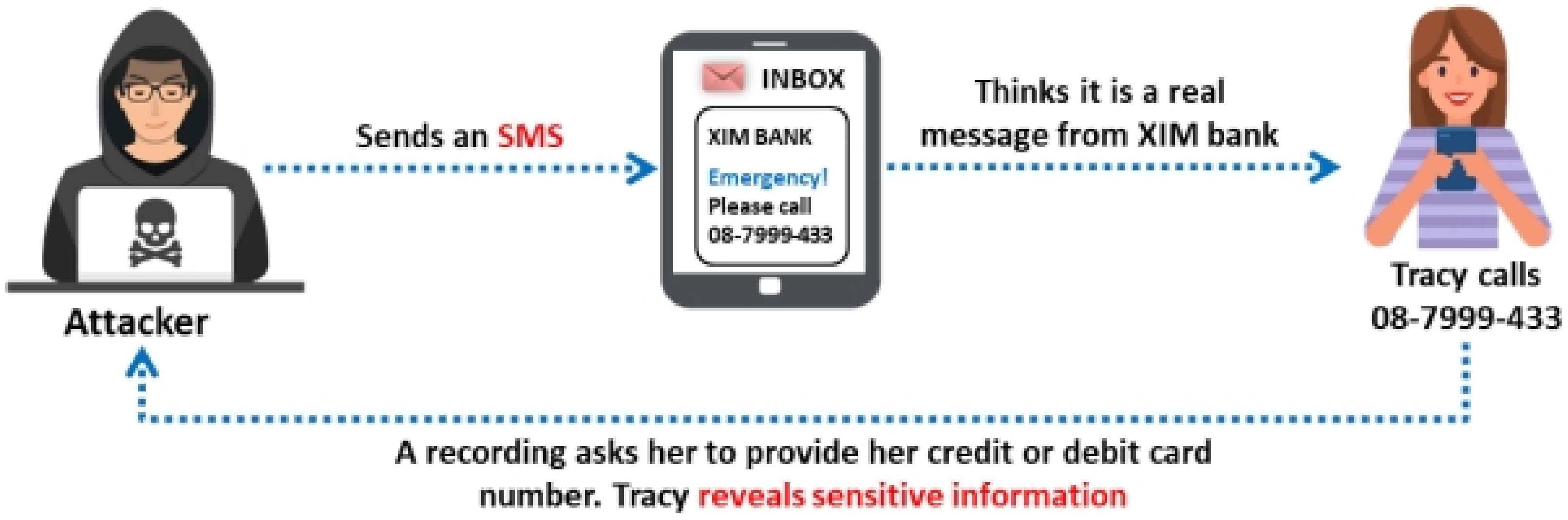
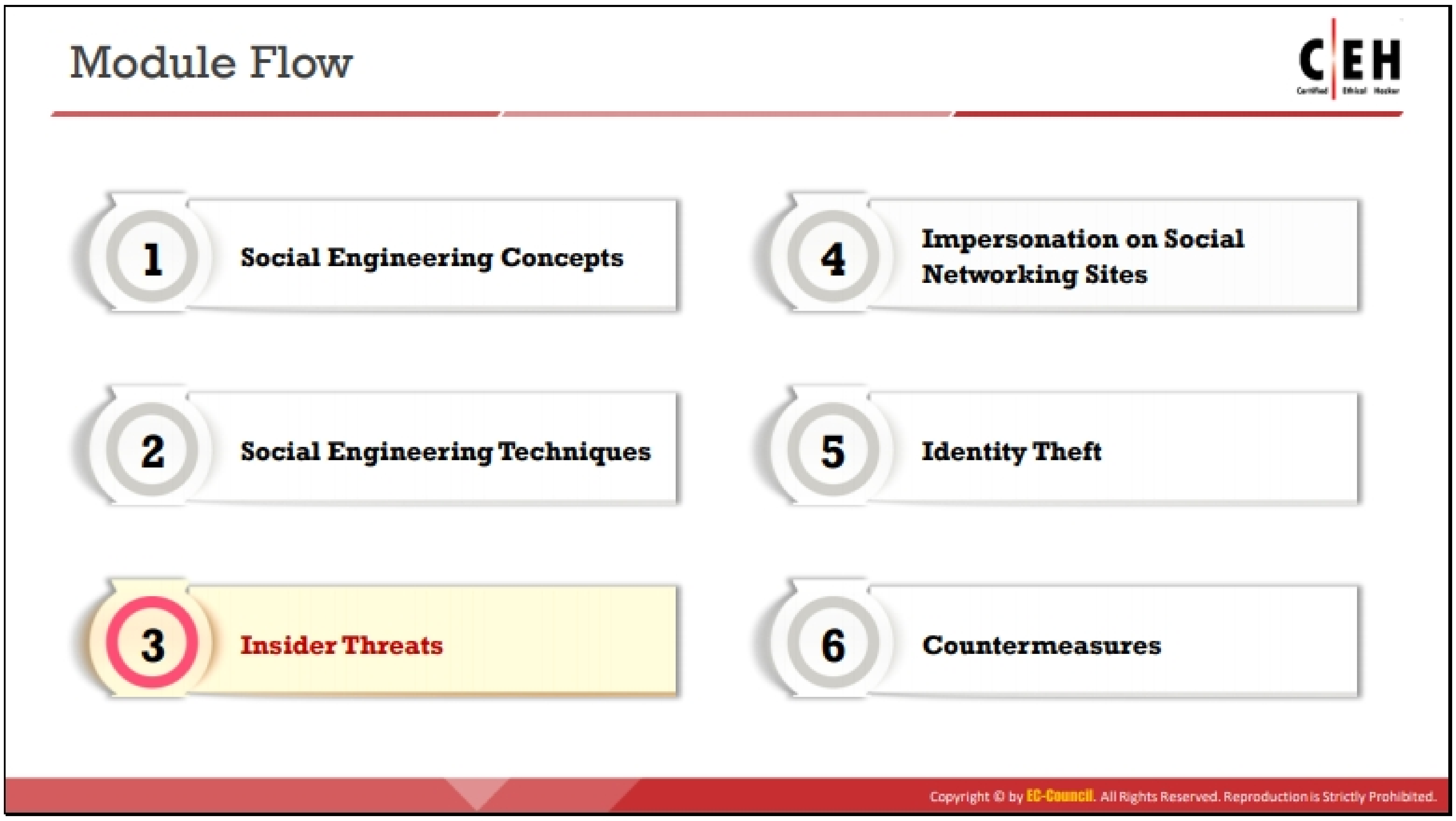
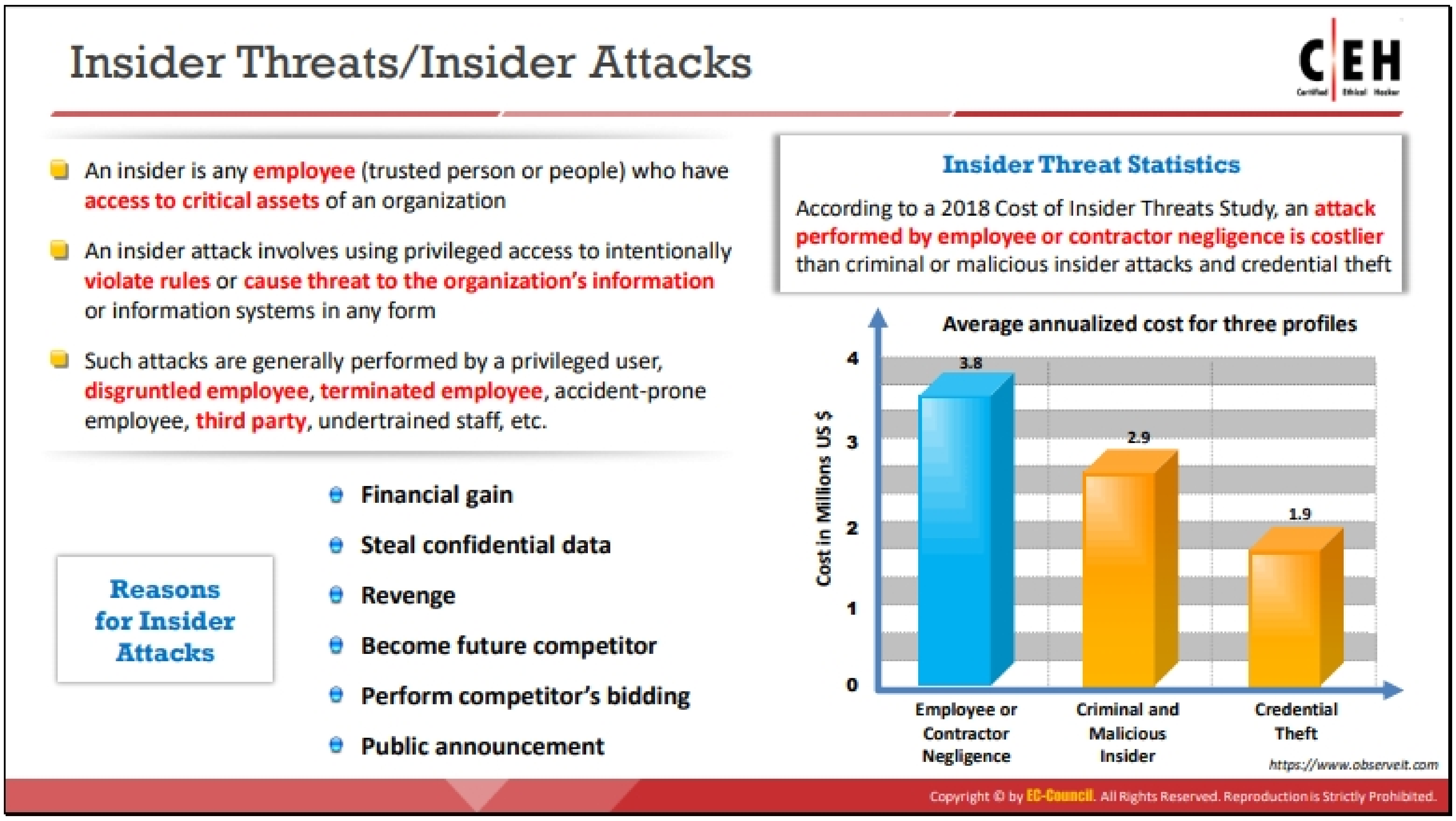

Sends an SMS
INBOX
XIM BANK
Emergency!
Please call
08-7999-433
Thinks it is a real message from XIM bank
Attacker
Tracy calls
08-7999-433
A recording asks her to provide her credit or debit card number. Tracy reveals sensitive information

Figure 9.11: SMiShing (SMS Phishing)



Module Flow

1. **Social Engineering Concepts**
2. **Social Engineering Techniques**
3. **Insider Threats**
4. **Impersonation on Social Networking Sites**
5. **Identity Theft**
6. **Countermeasures**



Insider Threats/Insider Attacks

- An insider is any **employee** (trusted person or people) who have **access to critical assets** of an organization
- An insider attack involves using privileged access to intentionally **violate rules** or **cause threat to the organization's information** or information systems in any form
- Such attacks are generally performed by a privileged user, **disgruntled employee**, **terminated employee**, accident-prone employee, **third party**, undertrained staff, etc.

Reasons for Insider Attacks

- Financial gain
- Steal confidential data
- Revenge
- Become future competitor
- Perform competitor's bidding
- Public announcement

Insider Threat Statistics

According to a 2018 Cost of Insider Threats Study, an **attack performed by employee or contractor negligence is costlier** than criminal or malicious insider attacks and credential theft

Average annualized cost for three profiles
Cost in Millions US $
0
1
2
3
4
3.8
2.9
1.9
Employee or Contractor Negligence
Criminal and Malicious Insider
Credential Theft

https://www.observeit.com

Insider Threats

An insider is any employee (trusted person) who has access to the critical assets of an organization. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. Insider attacks may cause great loss to the company. Further, they are dangerous because they are easy to launch and difficult to detect.

Insider attacks are generally performed by:

- **Privileged Users**: Attacks may come from the most trusted employees of the company, such as managers and system administrators, who have access to the company's confidential data and a higher probability of misusing the data, either intentionally or unintentionally.
- **Disgruntled Employees**: Attacks may come from unhappy employees or contract workers. Disgruntled employees, who intend to take revenge on the company, first acquire information and then wait for the right time to compromise the organization's resources.
- **Terminated Employees**: Some employees take valuable information about the company with them when terminated. These employees access the company's data after termination using backdoors, malware, or their old credentials if they are not disabled.
- **Accident-Prone Employees**: If an employee accidentally loses their mobile device, sends an email to incorrect recipients, or leaves a system loaded with confidential data logged-in, it can lead to unintentional data disclosure.
- **Third Parties**: Third parties, like remote employees, partners, dealers, and vendors, have access to the company's information. However, the security of their systems is unpredictable and could be a source of information leaks.
- **Undertrained Staff**: A trusted employee becomes an unintentional insider due to a lack of cybersecurity training. They fail to adhere to cybersecurity policies, procedures, guidelines, and best practices.

Companies in which insider attacks are common include credit card companies, health-care companies, network service providers, as well as financial and exchange service providers.

Reasons for Insider Attacks

- **Financial Gain**

  An attacker performs an insider attack mainly for financial gain. The insider sells the company's sensitive information to its competitor, steals a colleague's financial details for personal use, or manipulates the company's financial records or that of its personnel.

- **Steal Confidential Data**

  A competitor may inflict damage upon the target organization, steal critical information, or even put them out of business just by finding a job opening, preparing someone to get through the interview, and having that person hired by the competitor.

- **Revenge**

  It only takes one disgruntled person to seek revenge, and the company is compromised. Attacks may come from unhappy employees or contract workers with negative opinions about the company.

- **Become Future Competitor**

  Current employees may plan to start their own competing business and, by using the company's confidential data, these employees may access the system to steal or alter the company's client list.

- **Perform Competitors Bidding**

  Due to corporate espionage, even the most honest and trustworthy employees can be coerced into revealing the company's critical information through bribery or blackmail.

- **Public Announcement**

  A disgruntled employee may want to make a political or social statement and so leaks or damages the company's confidential data.

Insider Threat Statistics

Source: *https://www.observeit.com*

Although malicious intent is a serious factor for organizational security, according to a 2018 Cost of Insider Threats Study, an attack caused by employee or contractor negligence is costlier than theft and credential theft by a criminal or malicious insider:

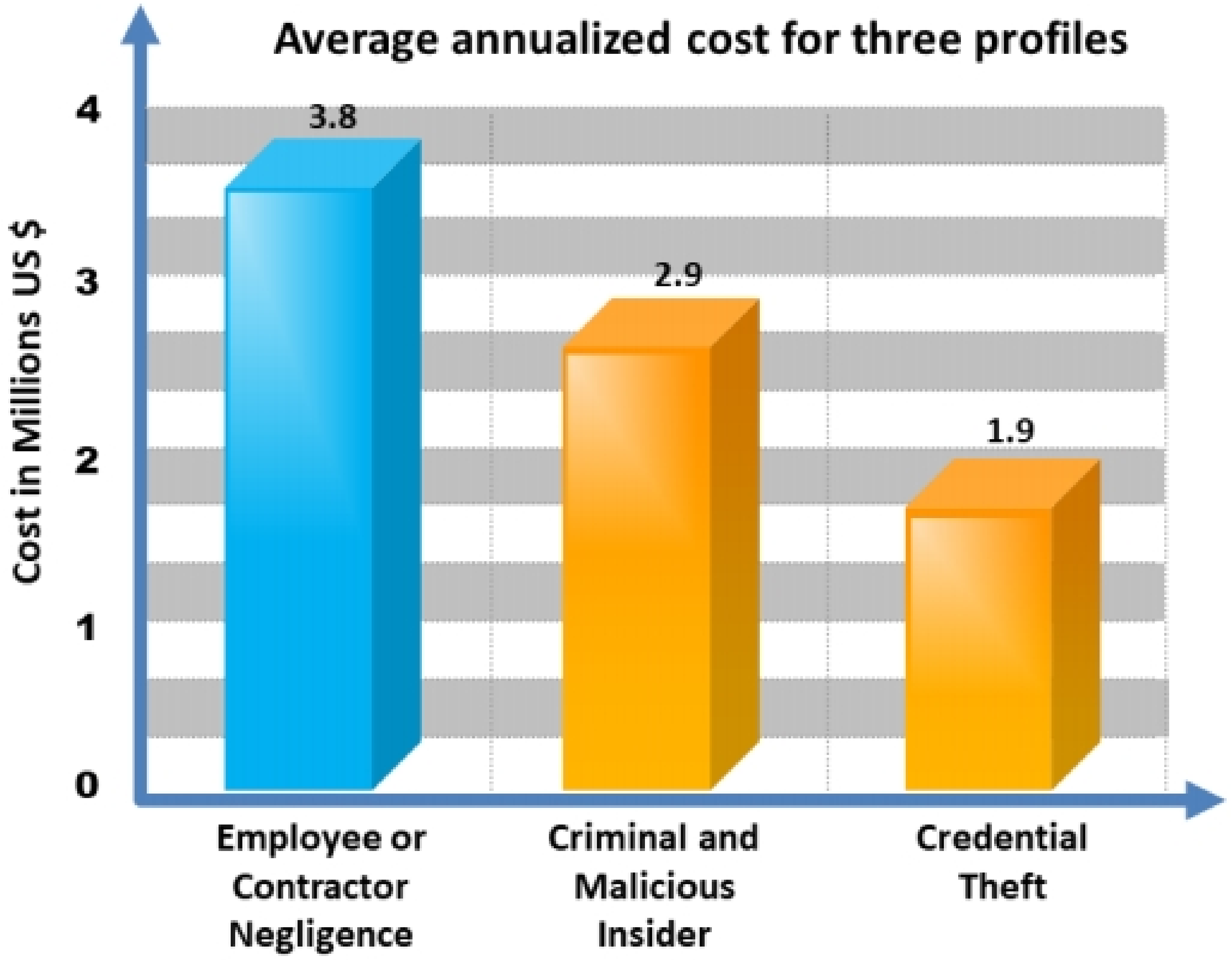
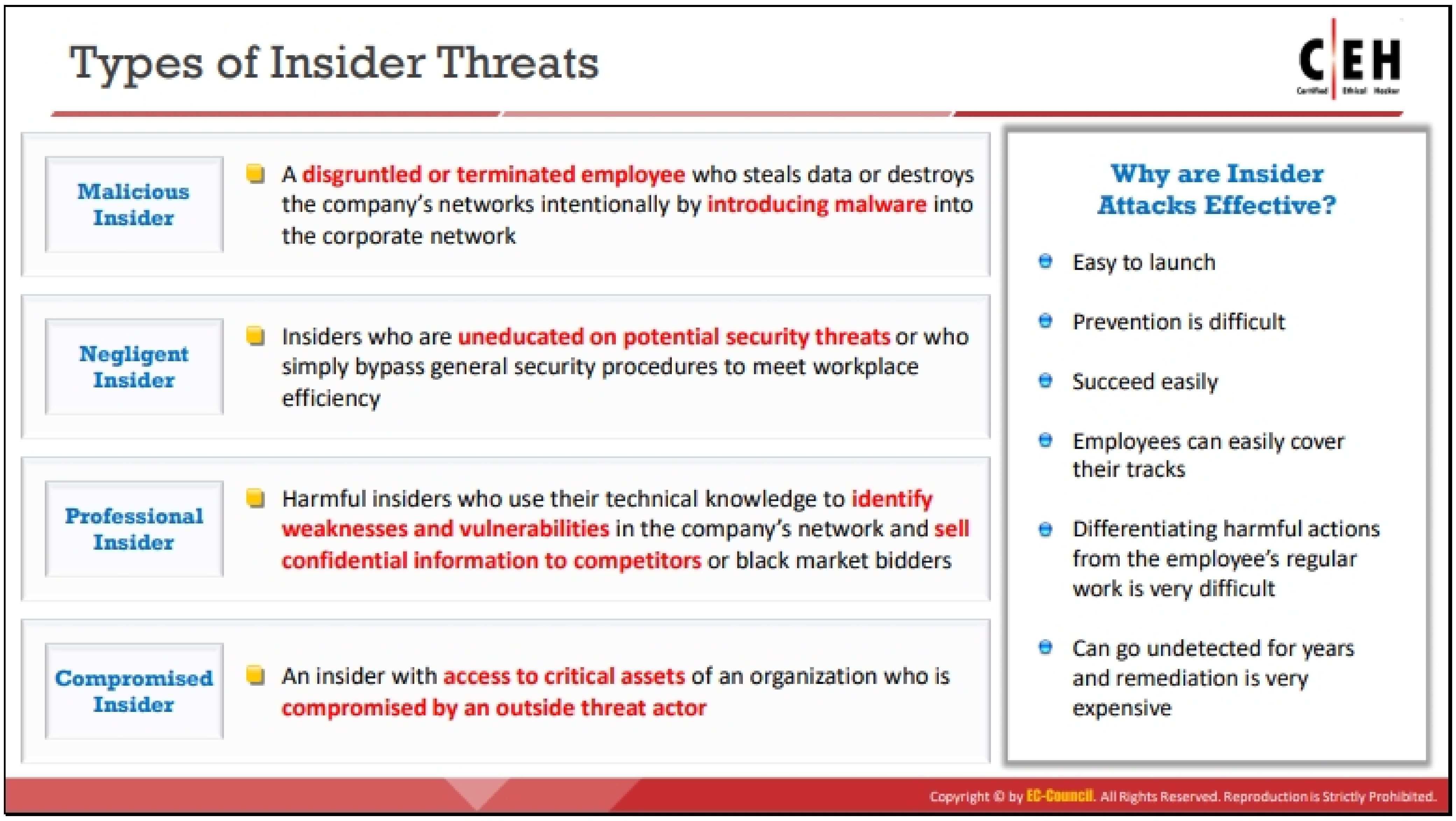


Figure 9.12: Graph Showing Insider Threat Statistics



Types of Insider Threats

Malicious Insider
- A disgruntled or terminated employee who steals data or destroys the company's networks intentionally by introducing malware into the corporate network

Negligent Insider
- Insiders who are uneducated on potential security threats or who simply bypass general security procedures to meet workplace efficiency

Professional Insider
- Harmful insiders who use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell confidential information to competitors or black market bidders

Compromised Insider
- An insider with access to critical assets of an organization who is compromised by an outside threat actor

Why are Insider Attacks Effective?
- Easy to launch
- Prevention is difficult
- Succeed easily
- Employees can easily cover their tracks
- Differentiating harmful actions from the employee's regular work is very difficult
- Can go undetected for years and remediation is very expensive

Types of Insider Threats

There are four types of insider threats. They are:

- **Malicious Insider**

  Malicious insider threats come from disgruntled or terminated employees who steal data or destroy company networks intentionally by injecting malware into the corporate network.

- **Negligent Insider**

  Insiders, who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency, are more vulnerable to social engineering attacks. Many insider attacks result from employee's laxity towards security measures, policies, and practices.

- **Professional Insider**

  Professional insiders are the most harmful insiders. They use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell the organization's confidential information to competitors or black-market bidders.

- **Compromised Insider**

  An outsider compromises an insider who has access to the critical assets or computing devices of an organization. This type of threat is more difficult to detect since the outsider masquerades as a genuine insider.

Why are Insider Attacks Effective?

Insider attacks are effective because:

- Insider attacks can go undetected for years, and remediation is expensive.
- Insider attacks are easy to launch.
- Preventing insider attacks is difficult; an inside attacker can easily succeed
- It is very difficult to differentiate harmful actions from the employee's regular work. It is hard to identify whether employees are performing malicious activities or not.
- Even after malicious activity is detected, the employee may refuse to accept responsibility and claim it was a mistake.
- It is easy for employees to cover their actions by editing or deleting logs to hide their malicious activities.

Example of Insider Attack: Disgruntled Employee

Most cases of insider abuse can be traced to individuals who are introverts, incapable of managing stress, experiencing conflict with management, frustrated with their job or office politics, craving respect or promotion, transferred, demoted, or issued an employment termination notice, among other reasons. Disgruntled employees may pass company secrets and intellectual property to competitors for monetary gain, thus harming the organization.

Disgruntled employees can use steganography programs to hide company secrets and later send the information to competitors as an innocuous-looking message such as a picture, image, or sound file using a work email account. No one suspects them because the attacker hides the stolen sensitive information in the picture or image file.

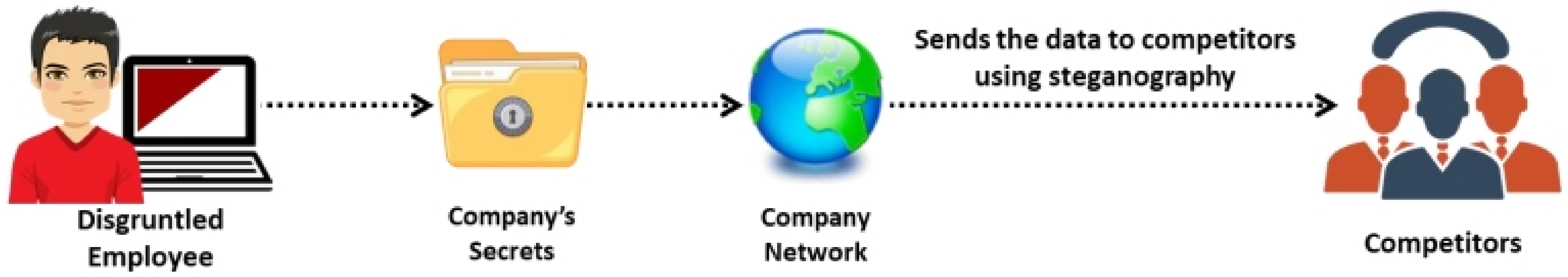
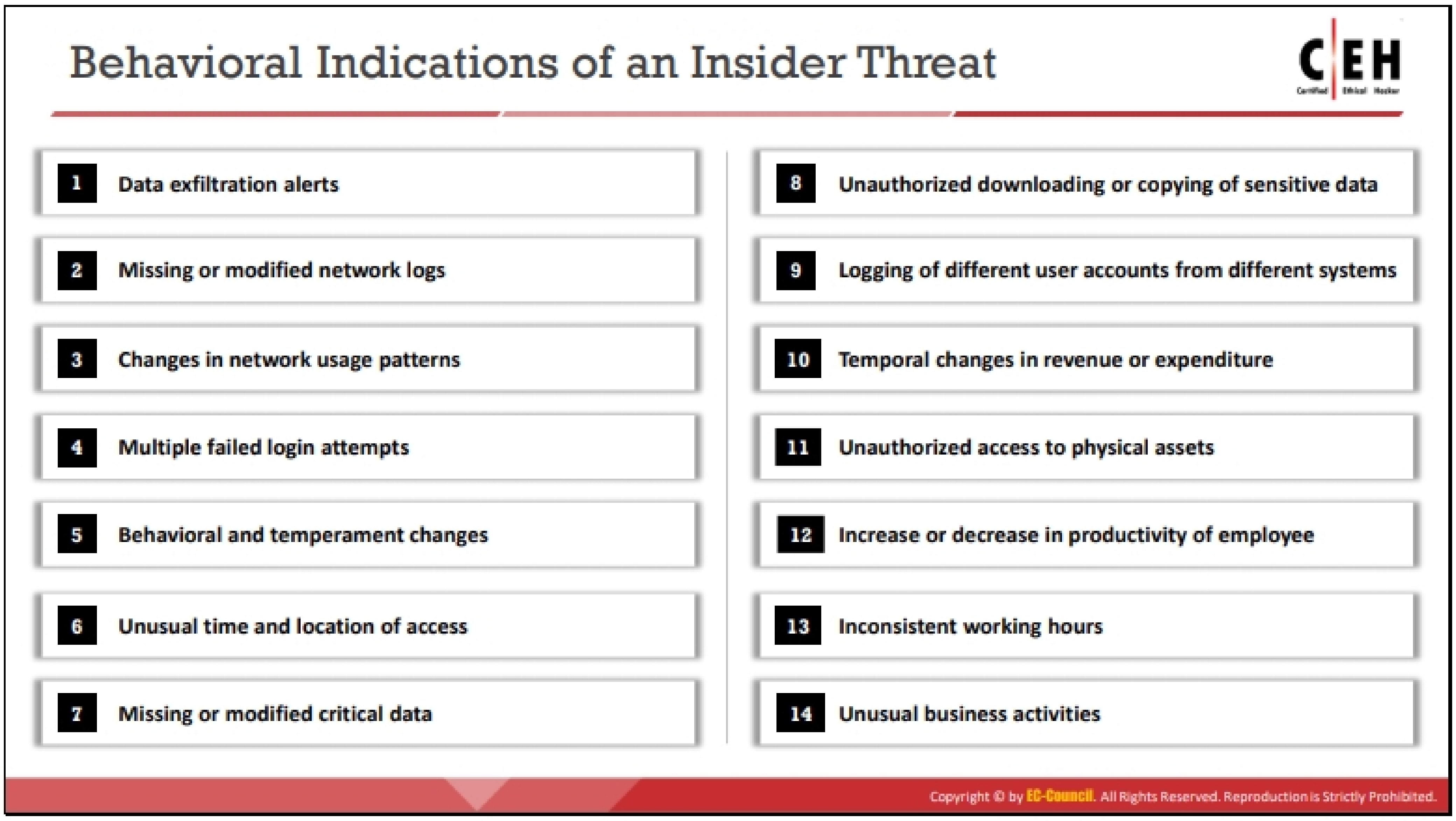


Figure 9.13: Example of Insider Attack — Disgruntled Employee



Behavioral Indications of an Insider Threat

1. Data exfiltration alerts
2. Missing or modified network logs
3. Changes in network usage patterns
4. Multiple failed login attempts
5. Behavioral and temperament changes
6. Unusual time and location of access
7. Missing or modified critical data
8. Unauthorized downloading or copying of sensitive data
9. Logging of different user accounts from different systems
10. Temporal changes in revenue or expenditure
11. Unauthorized access to physical assets
12. Increase or decrease in productivity of employee
13. Inconsistent working hours
14. Unusual business activities

Behavioral Indications of an Insider Threat

Indicators of insider threats are generally abnormal user activities that deviate from regular work activities. These represent unusual patterns of user behavior that require further analysis to identify malicious motives and intents. The most common indicator of insider threat is a lack of employee awareness about security measures.

The following are various behavioral indicators of insider threats:

- **Alerts of Data Exfiltration**

  Alerts of the unauthorized gathering and transmission of data on the network can represent an insider or malware attack. Insiders can also use paper, fax machines, hard drives, portable devices, and other computing equipment to gather and transfer sensitive data.

- **Missing or Modified Network Logs**

  Insiders try to access the log files to delete, modify, and edit unauthorized access events, file transfer logs, and other records from systems and network devices to avoid detection. Alerts of log modification, deletion, or access can indicate attacks.

- **Changes in Network Usage Patterns**

  Changes in the network patterns of the network-specific protocols, size of the packets, sources and destinations, frequency of user application sessions, and bandwidth usage can indicate malicious activity.

- **Multiple Failed Login Attempts**

  The insider can try to log in to unauthorized systems or applications by brute-force. So, multiple failed attempts may indicate an insider threat.

- **Behavioral and Temporal Changes**

  Deviation from established behavior and temporal changes in employee behavior such as spending capacity, frequent travel, anger management issues, constant quarrels with colleagues, and lethargy in performing work are some of the fraud indicators.

- **Unusual Time and Location of Access**

  Any mismatch in the timeline of an event can be suspicious and may indicate an insider threat. For example, if activities are logged on employee systems in their absence.

- **Missing or Modified Critical Data**

  Disgruntled employees can modify or delete sensitive data to damage the reputation of the organization.

- **Unauthorized Download or Copying of Sensitive Data**

  Insiders use legitimate and malicious tools to extract data from the organization's perimeter. Insiders can install malware, trojans, and backdoors to steal information.

- **Sending Sensitive Information to Personal Email Account**

  Insiders may send critical organizational information to their personal email accounts with malicious intent.

- **Logging of Different User Accounts from Different Systems**

  Unusual times of access combined with a change in the IP address of the system used to log into the account may represent malicious activities.

- **Temporal Changes in Revenue or Expenditure**

  Unexpected and unexplained changes in the financial status of an employee signify an income generated from external sources. The organization should audit their financial reports to identify whether the employee was involved in any malicious activities.

- **Unauthorized Access to Physical Assets**

  Activities such as employees using authorized assets without authentication, trying to escalate their privileges beyond their job requirements, or trying to gain physical access to the assets can represent a threat.

- **Increase or Decrease in Productivity of Employee**

  Employees who are unproductive, threatening, have legitimate or illegitimate job concerns, and disagree with intellectual property rights tend to be suspicious. A sudden increase or decrease in their productivity can signify suspicious behavior.

- **Inconsistent Working Hours, Unusual Business Activities, and Concealed or Frequent Foreign Trips**

  Employees with suspicious business activities like unusual login times, unusual office hours, unauthorized browsing and downloads, concealed trips abroad, and meetings with representatives from other countries or organizations may pose a threat to the organization.

- **Extreme Behavior Due to Mental Instability**

  Some employees possess unpredictable and extreme behavior, such as kleptomania, and a sudden change in behavior may be due to mental instability. This raises the probability that they will perform financial fraud, data theft, or physical theft.

- **Signs of vulnerability (Such as Drug or Alcohol Abuse, Financial Difficulties, Gambling, Illegal Activities)**

  Employees with bad habits such as drugs, gambling, and alcohol abuse, and relationship issues, may take a chance to breach the organization's data for money. Organizations must regularly monitor the activities of such employees.

- **Complaint on Sensitive Data Leak**

  Information or complaints regarding sensitive data leaks can represent an insider attack. Check for customer reviews and concerns to identify anomalies and analyze them to identify the insider.

- **Abnormal Access of Systems and User Accounts**

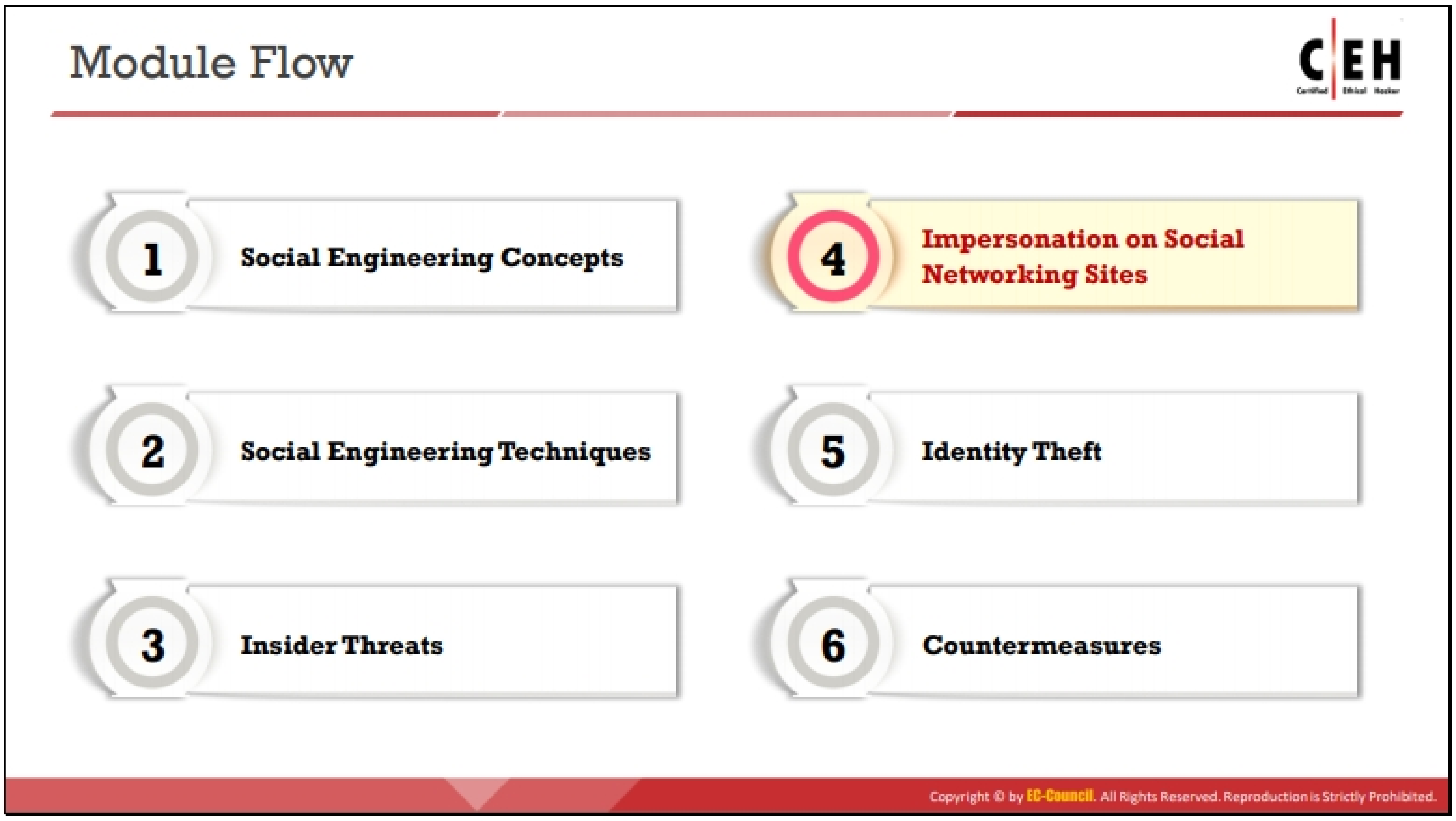
  The mismatch between the systems assigned and user accounts used to access the systems may indicate an insider threat.

- **Irresponsible Social Media Behavior**

  Insiders may attempt to create a negative impact on the organization by posting unnecessary information on social media websites.

- **Attempt to Access Restricted Zones**

  Employees with malicious intent may try to access restricted areas of the organization to collect sensitive information.



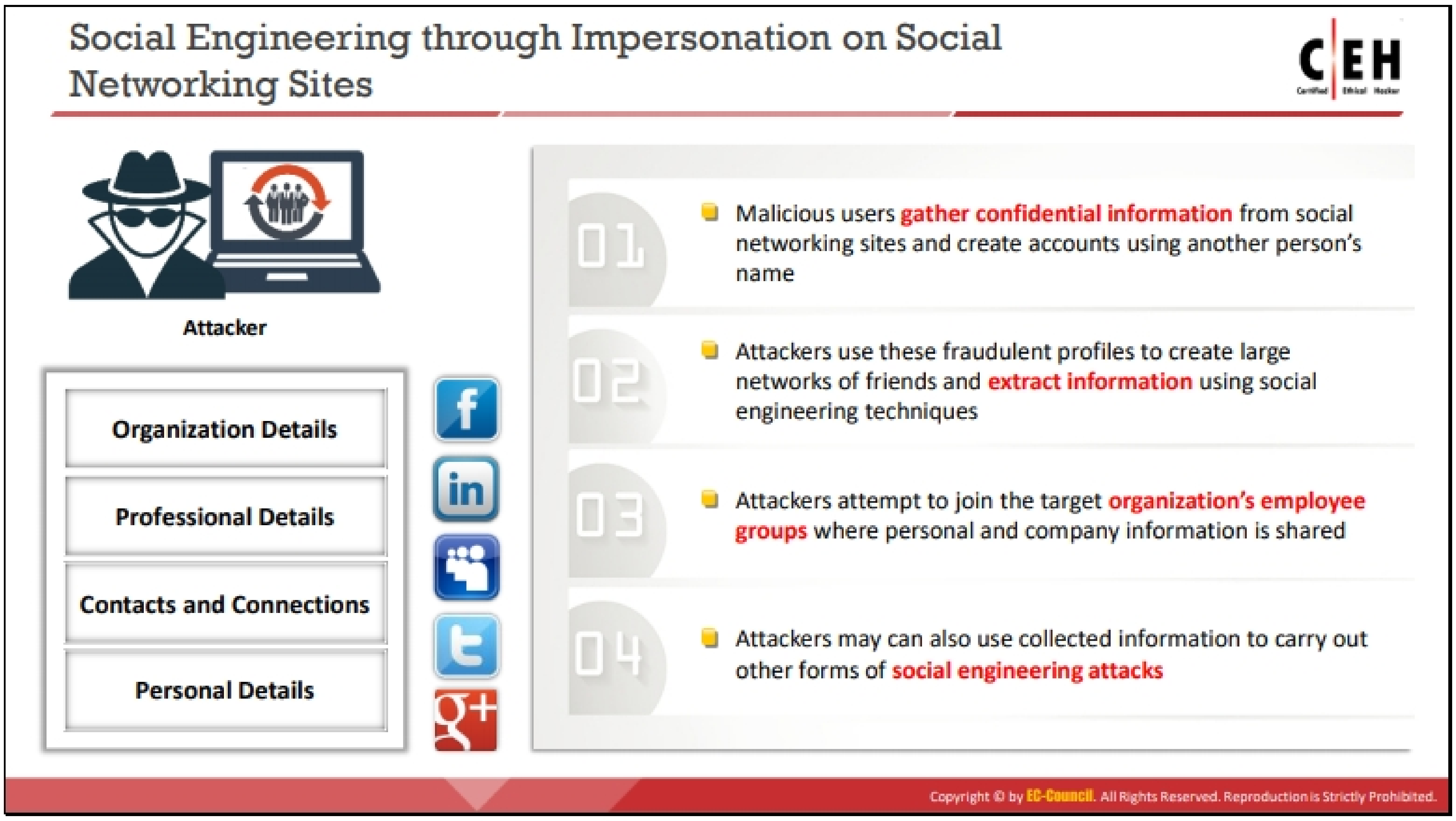
Module Flow

1 Social Engineering Concepts
2 Social Engineering Techniques
3 Insider Threats
4 Impersonation on Social Networking Sites
5 Identity Theft
6 Countermeasures

Impersonation on Social Networking Sites

Today social networking sites are widely used by many people that allow them to build online profiles, share information and media such as pictures, blog entries, and music clips. Thus, it is relatively easier for an attacker to impersonate someone. The victim is likely to trust the attacker and eventually reveal information that would help them gain access to the system.

This section describes how attackers perform social engineering through impersonation using various social networking sites such as Facebook, LinkedIn, and Twitter, and highlights the risks these sites pose to corporate networks.



Social Engineering through Impersonation on Social Networking Sites

Organization Details

Professional Details

Contacts and Connections

Personal Details

01
- Malicious users **gather confidential information** from social networking sites and create accounts using another person's name

02
- Attackers use these fraudulent profiles to create large networks of friends and **extract information** using social engineering techniques

03
- Attackers attempt to join the target **organization's employee groups** where personal and company information is shared

04
- Attackers may can also use collected information to carry out other forms of **social engineering attacks**

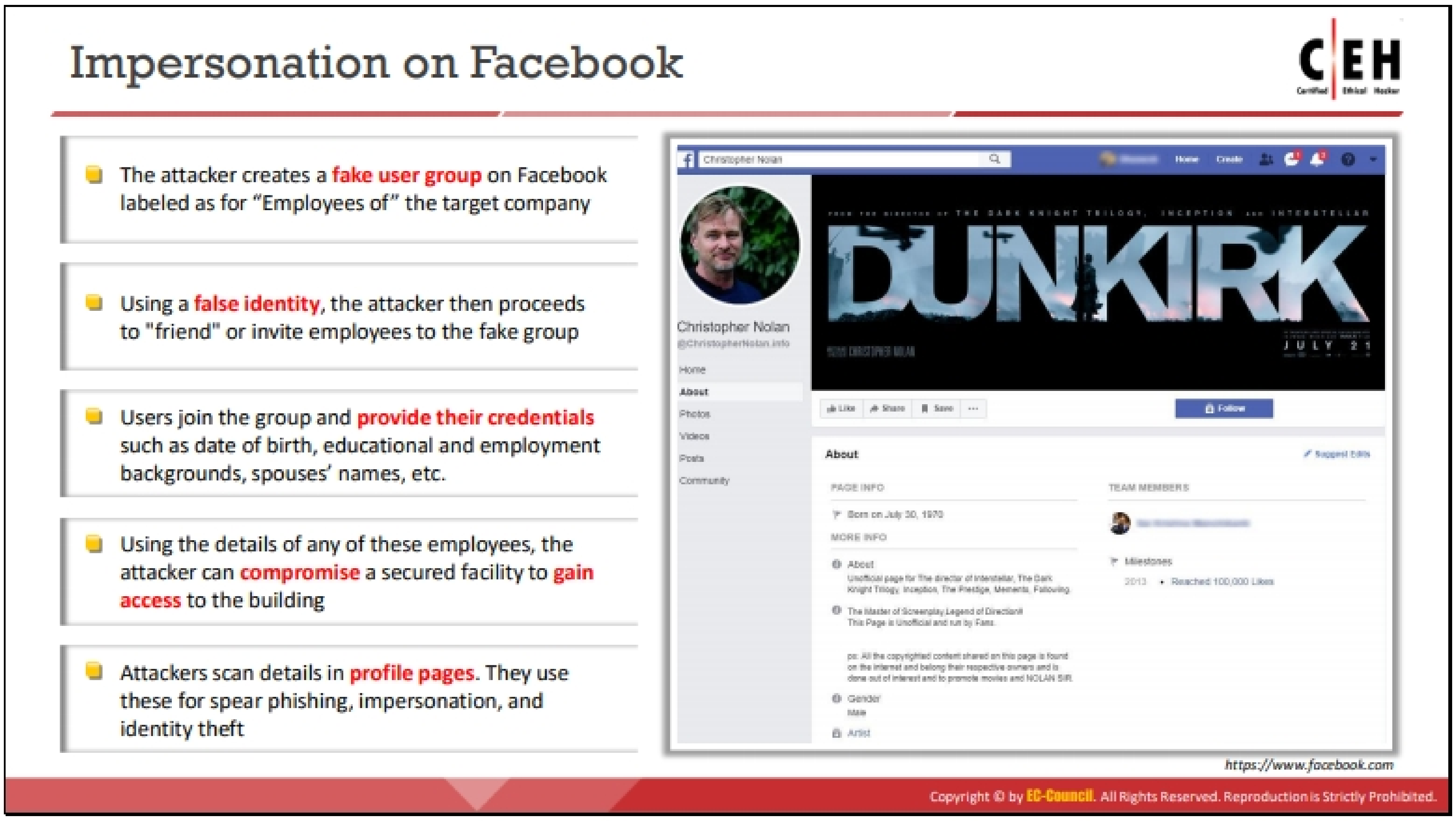
Social Engineering through Impersonation on Social Networking Sites

As social networking sites such as Facebook, Twitter, and LinkedIn are widely used, attackers coopt them as a vehicle for impersonation. There are two ways an attacker can perform impersonation on social networking sites:

- By creating a fictitious profile of the victim on the social media site
- By stealing the victim's password or indirectly gaining access to the victim's social media account

Social networking sites are a treasure trove for attackers because people share their personal and professional information on these sites, such as name, address, mobile number, date of birth, project details, job designation, company name, and location. The more information people share on a social networking site, the more likely it is that an attacker can impersonate them to launch attacks against them, their associates, or their organization. They may also try to join the target organization's employee groups to extract corporate data.

In general, the information attackers gather from social networking sites includes organization details, professional details, contacts and connections, and personal details, which they then use to execute other forms of social engineering attacks.



Impersonation on Facebook

- The attacker creates a **fake user group** on Facebook labeled as for "Employees of" the target company
- Using a **false identity**, the attacker then proceeds to "friend" or invite employees to the fake group
- Users join the group and **provide their credentials** such as date of birth, educational and employment backgrounds, spouses' names, etc.
- Using the details of any of these employees, the attacker can **compromise** a secured facility to **gain access** to the building
- Attackers scan details in **profile pages**. They use these for spear phishing, impersonation, and identity theft

Christopher Nolan
@ChristopherNolan.info

About

PAGE INFO

Born on July 30, 1970

MORE INFO

About
Unofficial page for The director of Interstellar, The Dark Knight Trilogy, Inception, The Prestige, Memento, Following.

The Master of Screenplay Legend of Direction!!
This Page is Unofficial and run by Fans.

ps: All the copyrighted content shared on this page is found on the internet and belong their respective owners and is done out of interest and to promote movies and NOLAN SIR.

Gender
Male

Artist

TEAM MEMBERS

[redacted]

Milestones
2013 • Reached 100,000 Likes

https://www.facebook.com

Impersonation on Facebook

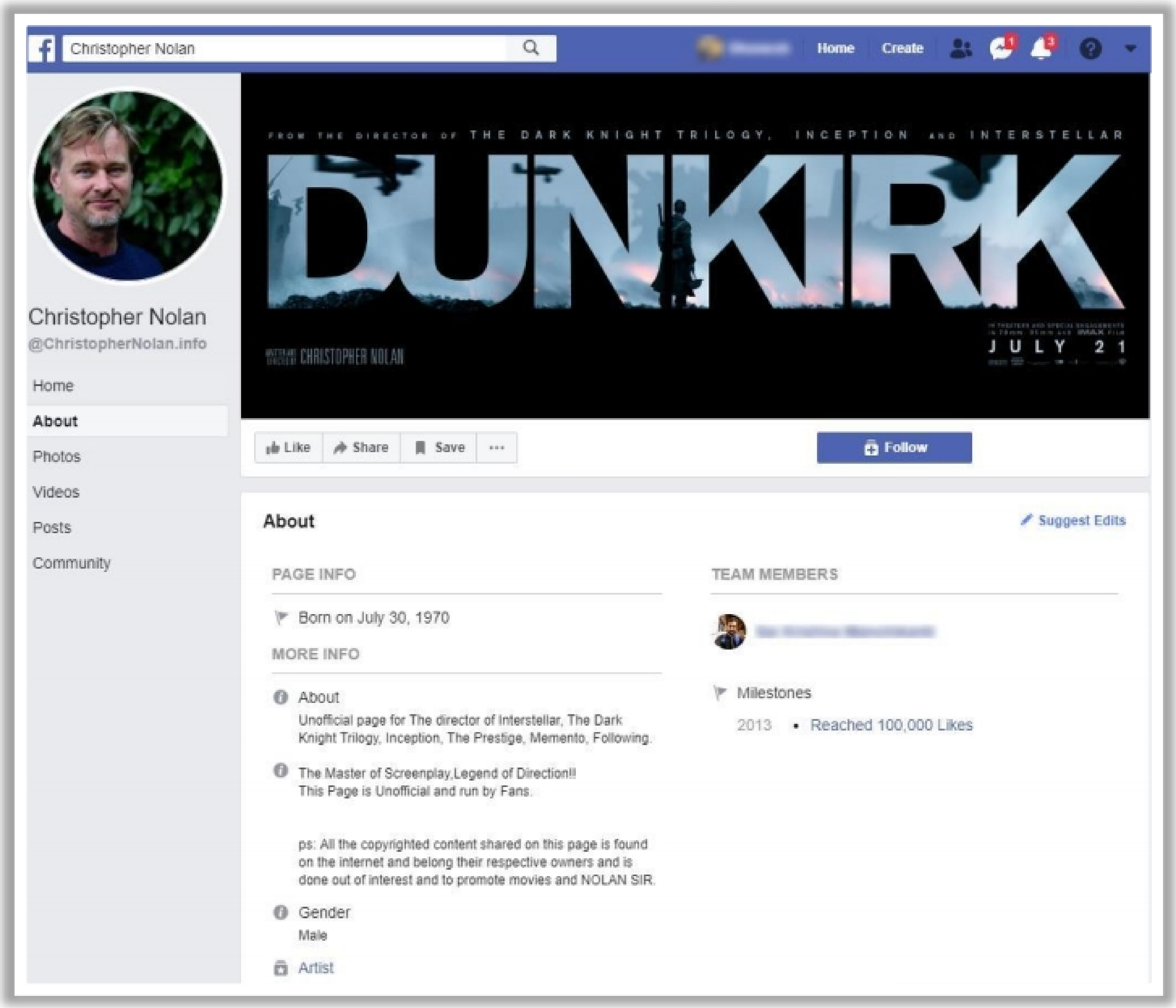
Source: *https://www.facebook.com*

Facebook is a well-known social networking site that connects people. It is widely used between friends who share comments and upload photos, links, and videos. To impersonate users on Facebook, attackers use nicknames or aliases instead of their real names. They create fake accounts and try to add "**Friends**" to view others' profiles and obtain critical and valuable information.

The steps an attacker takes to lure a victim into revealing sensitive information:

- Create a fake user group on Facebook identified as "Employees of" the target company
- Using a false identity, proceed to "friend," or invite actual employees to the fake group, "Employees of Company XYZ"
- Users join the group and provide their credentials such as date of birth, educational and employment backgrounds, or spouses' names.
- Using the details of any one of the employees, an attacker can compromise a secured facility to gain access to the building

Attackers create a fake account and scan the details on the profile pages of various targets on social networking sites such as LinkedIn and Twitter to engage in spear phishing, impersonation, and identity theft.


Christopher Nolan
[redacted]
Home
Create
FROM THE DIRECTOR OF THE DARK KNIGHT TRILOGY, INCEPTION AND INTERSTELLAR
DUNKIRK
CHRISTOPHER NOLAN
JULY 21
Christopher Nolan
@ChristopherNolan.info
Home
About
Photos
Videos
Posts
Community
Like
Share
Save
···
Follow
Suggest Edits

About

PAGE INFO

Born on July 30, 1970

MORE INFO

About
Unofficial page for The director of Interstellar, The Dark Knight Trilogy, Inception, The Prestige, Memento, Following.

The Master of Screenplay,Legend of Direction!!
This Page is Unofficial and run by Fans.

ps: All the copyrighted content shared on this page is found on the internet and belong their respective owners and is done out of interest and to promote movies and NOLAN SIR.

Gender
Male

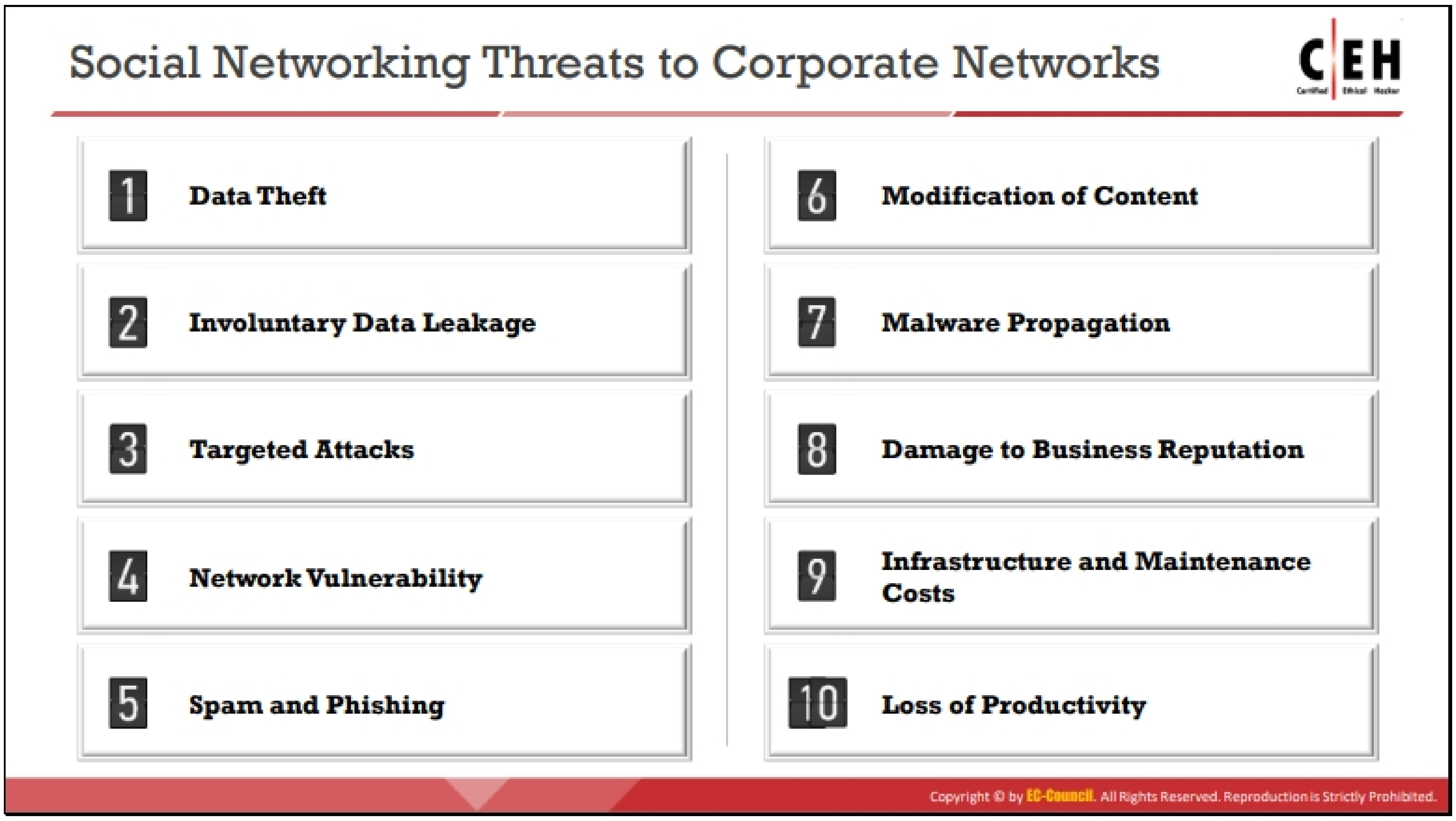
Artist

TEAM MEMBERS

[redacted]

Milestones
2013 • Reached 100,000 Likes

Figure 9.14: Screenshot showing Facebook profile



Social Networking Threats to Corporate Networks

1. Data Theft
2. Involuntary Data Leakage
3. Targeted Attacks
4. Network Vulnerability
5. Spam and Phishing
6. Modification of Content
7. Malware Propagation
8. Damage to Business Reputation
9. Infrastructure and Maintenance Costs
10. Loss of Productivity

Social Networking Threats to Corporate Networks

Before sharing data on a social networking site, or enhancing their channels, groups, or profiles, private and corporate users should be aware of the following social or technical security risks:

- **Data Theft**: Social networking sites are huge databases accessed by many people worldwide, increasing the risk of information exploitation.
- **Involuntary Data Leakage**: In the absence of a strong policy that sets clear lines between personal and corporate content, employees may unknowingly post sensitive data about their company on social networking sites, which might help an attacker to launch an attack on the target organization.
- **Targeted Attacks**: Attackers use the information posted on social networking sites to launch targeted attacks on specific users or companies.
- **Network Vulnerability**: All social networking sites are subject to flaws and bugs such as login issues and Java vulnerabilities, which attackers could exploit. This could, in turn, lead to the leakage of confidential information related to the target organization's network.
- **Spam and Phishing**: Employees using work e-mail IDs on social networking sites will probably receive spam and become targets of phishing attacks, which could compromise the organization's network.
- **Modification of Content**: In the absence of proper security measures and efforts to preserve identity, blogs, channels, groups, profiles, and other platforms can be spoofed or hacked.

- **Malware Propagation**: Social networking sites are ideal platforms for attackers to spread viruses, bots, worms, trojans, spyware, and other malware.
- **Business Reputation**: Attackers can falsify information about an organization or an employee on social networking sites, resulting in loss of reputation.
- **Infrastructure and Maintenance Costs**: Using social networking sites entails added infrastructure and maintenance resources for organizations to ensure that their defensive layers are effective safeguards.
- **Loss of Productivity**: Organizations must monitor employees’ network activities to maintain security and ensure that such activities do not misuse the system and company resources.

Module Flow

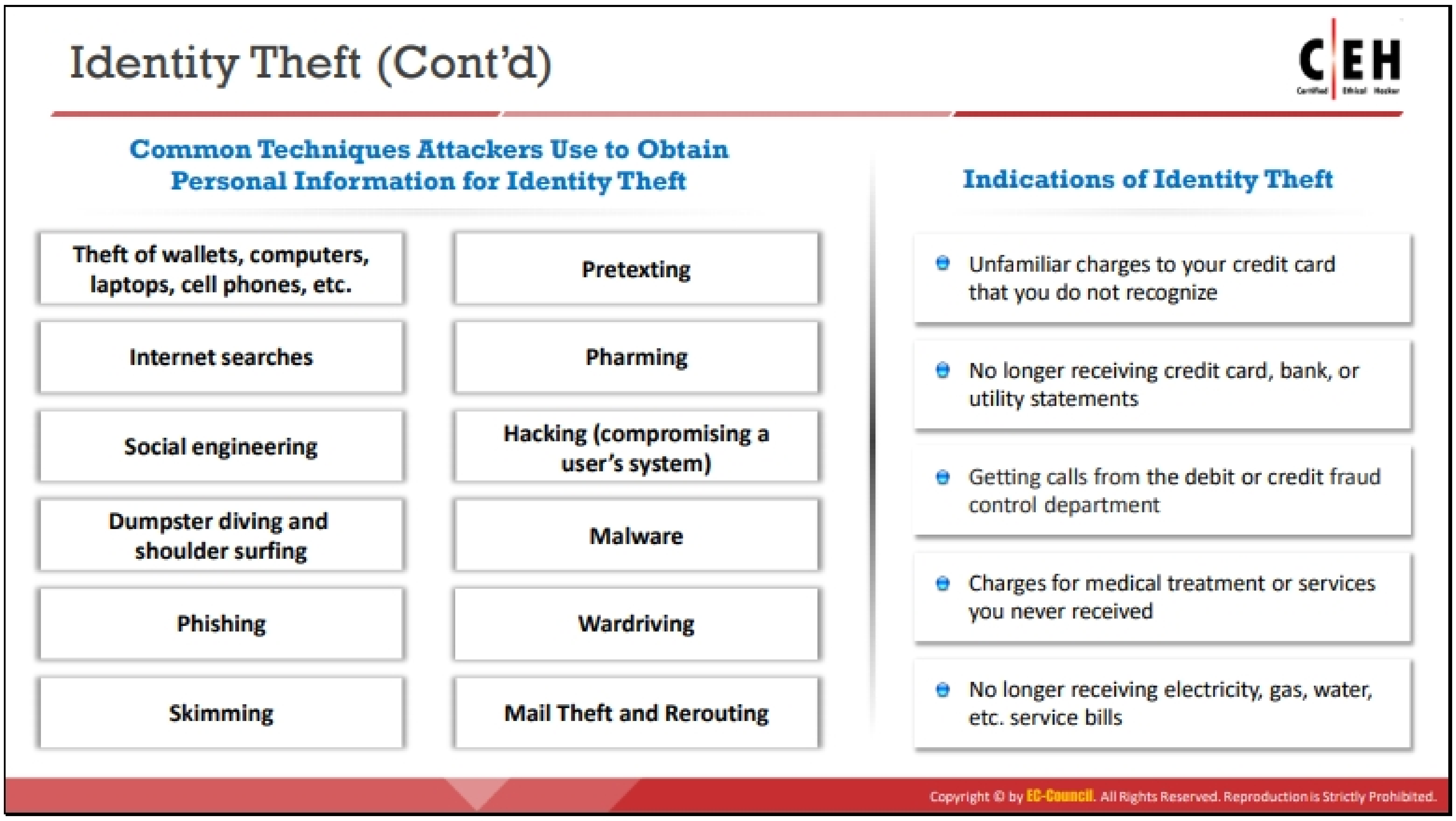
1. **Social Engineering Concepts**
2. **Social Engineering Techniques**
3. **Insider Threats**
4. **Impersonation on Social Networking Sites**
5. **Identity Theft**
6. **Countermeasures**

Identity Theft

- Identity theft is a crime in which **an imposter steals your personally identifiable information** such as name, credit card number, social security or driver's license numbers, etc. to commit fraud or other crimes
- Attackers can use identity theft to **impersonate employees of a target** organization and physically access facilities

Types of Identity Theft

- Child identity theft
- Criminal identity theft
- Financial identity theft
- Driver's license identity theft
- Insurance identity theft
- Medical identity theft
- Tax identity theft
- Identity cloning and Concealment
- Synthetic identity theft
- Social security identity theft



Identity Theft (Cont'd)

Common Techniques Attackers Use to Obtain Personal Information for Identity Theft

- Theft of wallets, computers, laptops, cell phones, etc.
- Internet searches
- Social engineering
- Dumpster diving and shoulder surfing
- Phishing
- Skimming
- Pretexting
- Pharming
- Hacking (compromising a user's system)
- Malware
- Wardriving
- Mail Theft and Rerouting

Indications of Identity Theft

- Unfamiliar charges to your credit card that you do not recognize
- No longer receiving credit card, bank, or utility statements
- Getting calls from the debit or credit fraud control department
- Charges for medical treatment or services you never received
- No longer receiving electricity, gas, water, etc. service bills

Identity Theft

Identity theft is a problem that many consumers face today. In the United States, some state legislators have imposed laws restricting employees from providing their SSNs (Social Security Numbers) during their recruitment. Identity theft frequently figures in news reports. Companies should be informed about identity theft so that they do not endanger their own anti-fraud initiatives.

This section discusses identity theft, including types of identity theft, common techniques attackers use to obtain personal information for identity theft, and various indications of identity theft.

The Identity Theft and Assumption Deterrence Act of 1998 defines identity theft as the illegal use of someone's identification. Identity theft occurs when someone steals others' personally identifiable information for fraudulent purposes. Attackers illegally obtain personally identifying information to commit fraud or other criminal acts.

Types of personally identifiable information stolen by identity thieves:

- Name
- Home and office address
- Social security number
- Phone number
- Date of birth
- Bank account number
- Credit card information
- Credit report
- Driving license number
- Passport number

The attacker steals people's identity for fraudulent purposes such as:

- To open new credit card accounts in the name of the user without paying the bills
- To open a new phone or wireless account in the user's name, or to run up charges on their existing account
- To use the victims' information to obtain utility services such as electricity, heating, or cable TV
- To open bank accounts with the intention of writing bogus checks using the victim's information
- To clone an ATM or debit card to make electronic withdrawals from the victim's accounts
- To obtain loans for which the victim is liable
- To obtain a driver's license, passport, or other official ID card that contains the victim's data with the attacker's photos
- Using the victim's name and Social Security number to receive their government benefits
- To impersonate an employee of a target organization to physically access its facility
- To take over the victim's insurance policies
- To sell the victim's personal information
- To order goods online using a drop-site
- To hijack email accounts
- To obtain health services
- To submit fraudulent tax returns
- To commit other crimes with the intention of providing the victim's name to the authorities during arrest, instead of their own

Types of Identity Theft

Identity theft is constantly increasing, and identity thieves are finding new ways or techniques to steal different types of target information. Some of the types of identity theft are as follows:

- **Child Identity Theft**

  This type of identity theft occurs when the identity of a minor is stolen. This is desirable because it may go undetected for a long time. After birth, parents apply for a Social Security Number for their child, which along with a different date of birth, is used by identity thieves to apply for credit accounts, loans or utility services, or to rent a place to live and apply for government benefits.

- **Criminal Identity Theft**

  This is one of the most common and most damaging types of identity theft. A criminal uses someone's identity to escape criminal charges. When they are caught or arrested, they provide the assumed identity. The best way to protect against criminal identity theft is to keep all personal information secure, which includes following safe Internet practices and being cautious of "shoulder surfers."

- **Financial Identity Theft**

  This type of identity theft occurs when a victim's bank account or credit card information is stolen and illegally used by a thief. They can max out a credit card and withdraw money from the account, or can use the stolen identity to open a new account, apply for new credit cards, and take out loans. The information that is required to hack into the victim's account and steal their information is obtained through viruses, phishing attacks, or data breaches.

- **Driver's License Identity Theft**

  This type of identity theft is the easiest as it requires a little sophistication. A person can lose their driver's license, or it can easily be stolen. Once it falls into the wrong hands, the perpetrator can sell the stolen driver's license or misuse it by committing traffic violations, of which the victim is unaware of and fails to pay fines for, ending up with their license suspended or revoked.

- **Insurance Identity Theft**

  Insurance identity theft is closely related to medical identity theft. It takes place when a perpetrator unlawfully takes the victim's medical information to access their insurance for medical treatment. Its effects include difficulties in settling medical bills, higher insurance premiums, and probable trouble in acquiring future medical coverage.

- **Medical Identity Theft**

  This is the most dangerous type of identity theft where the perpetrator uses the victim's name or information without the victim's consent or knowledge to obtain medical products and claim health insurance or healthcare services. Medical identity theft results in frequent erroneous entries in the victim's medical records, which could lead to false diagnoses and life-threatening decisions by the doctors.

- **Tax Identity Theft**

  This type of identity theft occurs when the perpetrator steals the victim's Social Security Number to file fraudulent tax returns and obtain fraudulent tax refunds. It creates difficulties for the victim in accessing their legitimate tax refunds and results in a loss of funds. Phishing emails are one of the main tricks used by the criminal to steal a target's information. Therefore, protection from such identity theft includes the adoption of safe Internet practices.

- **Identity Cloning and Concealment**

  This type of identity theft encompasses all forms of identity theft, where the perpetrators attempt to impersonate someone else simply in order to hide their identity. These perpetrators could be illegal immigrants, those hiding from creditors, or simply those who want to become "anonymous."

- **Synthetic Identity Theft**

  This is one of the most sophisticated types of identity theft, where the perpetrator obtains information from different victims to create a new identity. Firstly, he steals a Social Security Number and uses it with a combination of fake names, date of birth, address, and other details required for creating a new identity. The perpetrator uses this new identity to open new accounts, loans, credit cards, phones, other goods, and services.

- **Social Identity Theft**

  This is another common type of identity theft where the perpetrator steals victim's Social Security Number in order to derive various benefits such as selling it to an undocumented person, using it to defraud the government by getting a new bank account, loans, credit cards, or applying for and obtaining a new passport.

Common Techniques Attackers Use to Obtain Personal Information for Identity Theft

Discussed below are some of the methods by which attackers steal targets' identities, which in turn allow them to commit fraud and other criminal activities:

- **Theft of wallets, computers, laptops, cell phones, backup media, and other sources of personal information**

  Physical theft is common. Attackers steal hardware from places such as hotels and recreational places such as clubs, restaurants, parks, and beaches. Given adequate time, they can recover valuable data from these sources.

- **Internet Searches**

  Attackers can gather a considerable amount of sensitive information via legitimate Internet sites, using search engines such as Google, Bing, and Yahoo!.

- **Social Engineering**

  Social engineering is the art of manipulating people into performing certain actions or divulging personal information and accomplishing their task without using cracking methods.

- **Dumpster Diving and Shoulder Surfing**

  Attackers rummage through household garbage and the trash bins of organizations, ATM centers, hotels, and other places to obtain personal and financial information for fraudulent purposes.

Criminals may find user information by glancing at documents, observing personal identification numbers (PINs) typed into automatic teller machines (ATM), or by overhearing conversations.

- **Phishing**

  The "fraudster" may pretend to be from a financial institution or other reputable organization and send spam or pop-up messages to trick users into revealing their personal information.

- **Skimming**

  Skimming refers to stealing credit or debit card numbers by using special storage devices called skimmers or wedges when processing the card.

- **Pretexting**

  Fraudsters may impersonate executives from financial institutions, telephone companies, and other businesses. They rely on "smooth-talking" and win the trust of an individual to reveal sensitive information.

- **Pharming**

  Pharming, also known as domain spoofing, is an advanced form of phishing in which the attacker redirects the connection between the IP address and its target server. The attacker may use cache poisoning (modifying the Internet address to that of a rogue address) to do so. When the users type in the Internet address, it redirects them to a rogue website that resembles the original.

- **Hacking (compromising a user's system)**

  Attackers may compromise user systems and router information using listening devices such as sniffers and scanners. They gain access to an abundance of data, decrypt it (if necessary), and use it for identity theft.

- **Keyloggers and Password Stealers (Malware)**

  An attacker may infect the user's computer with trojans, viruses, or other malware and then record and collect the user's keystrokes to steal passwords, usernames, and other sensitive information of personal, financial, or business import.

  Attackers may also use emails to send fake forms, such as Internal Revenue Service (IRS) forms, to gather information from their victims.

- **Wardriving**

  Attackers search for unsecured Wi-Fi wireless networks in moving vehicles containing laptops, smartphones, or PDAs. Once they find unsecured networks, they access any sensitive information stored on the devices of the users on those networks.

- **Mail Theft and Rerouting**

  Often, mailboxes contain bank documents (credit cards or account statements), administrative forms, and other important correspondence. Criminals use this information to obtain credit card information or to reroute the mail to a new address.

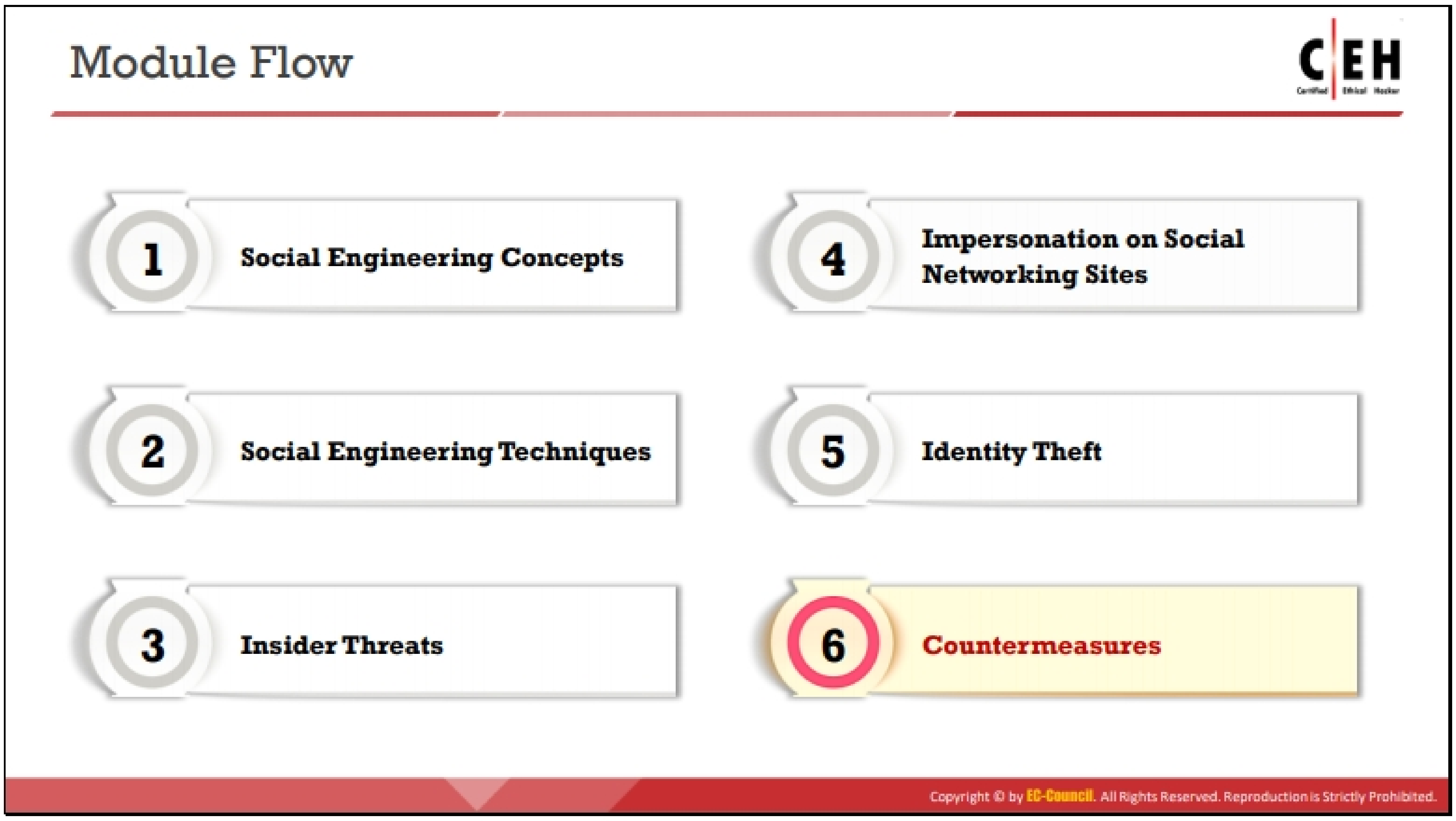
Indications of Identity Theft

People do not realize that they are the victim of identity theft until they experience some unknown and unauthorized issues as a result of the theft. Therefore, it is of paramount importance that people watch out for the warning signs that their identities have been compromised. Listed below are some of the signs of identity theft:

- Unfamiliar charges to your credit card that you do not recognize.
- No longer receive credit card, bank, or utility statements
- Creditors call asking about an unknown account on your name.
- There are numerous traffic violations under your name that you did not commit.
- You receive charges for medical treatment or services you never received.
- There is more than one tax return filed under your name.
- Being denied access to your own account and unable to take out loans or use other services.
- Not receiving electricity, gas, water, or other services bills due to stolen mail.
- Sudden changes in your personal medical records showing a condition you do not suffer from.

Some additional indications of identity theft are as follow:

- Getting a notification that your information was compromised or misused by a data breach in a company where you are an employee or have an account.
- An inexplicable cash withdrawal from your bank account.
- Calls from debit or credit card fraud control departments giving warnings about suspicious activities on your accounts.
- A refusal of government benefits to you and your child because those benefits are already being received by some other account using your child’s Social Security Number.
- Your medical insurance plan rejects your authentic medical claim because someone tampered with your medical records, causing you to reach your benefit limit.



Module Flow

1 **Social Engineering Concepts**

2 **Social Engineering Techniques**

3 **Insider Threats**

4 **Impersonation on Social Networking Sites**

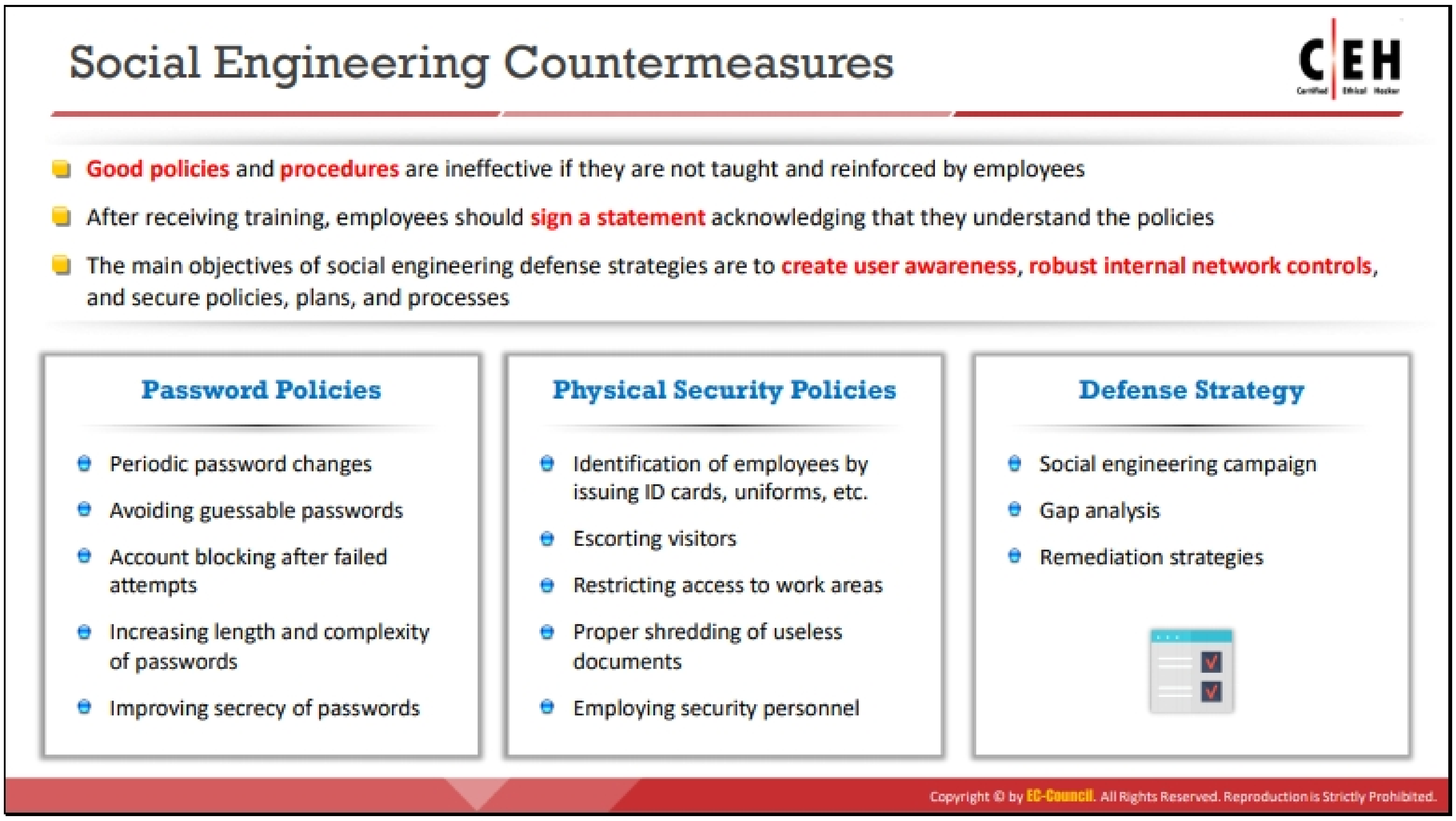
5 **Identity Theft**

6 **Countermeasures**

Countermeasures

Social engineers exploit human behavior (such as manners, enthusiasm toward work, laziness, or naivete) to gain access to the targeted company's information resources. Social engineering attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against social engineering attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

This section deals with countermeasures that an organization can implement to be more secure against social engineering attacks.



Social Engineering Countermeasures

- **Good policies** and **procedures** are ineffective if they are not taught and reinforced by employees
- After receiving training, employees should **sign a statement** acknowledging that they understand the policies
- The main objectives of social engineering defense strategies are to **create user awareness**, **robust internal network controls**, and secure policies, plans, and processes

Password Policies

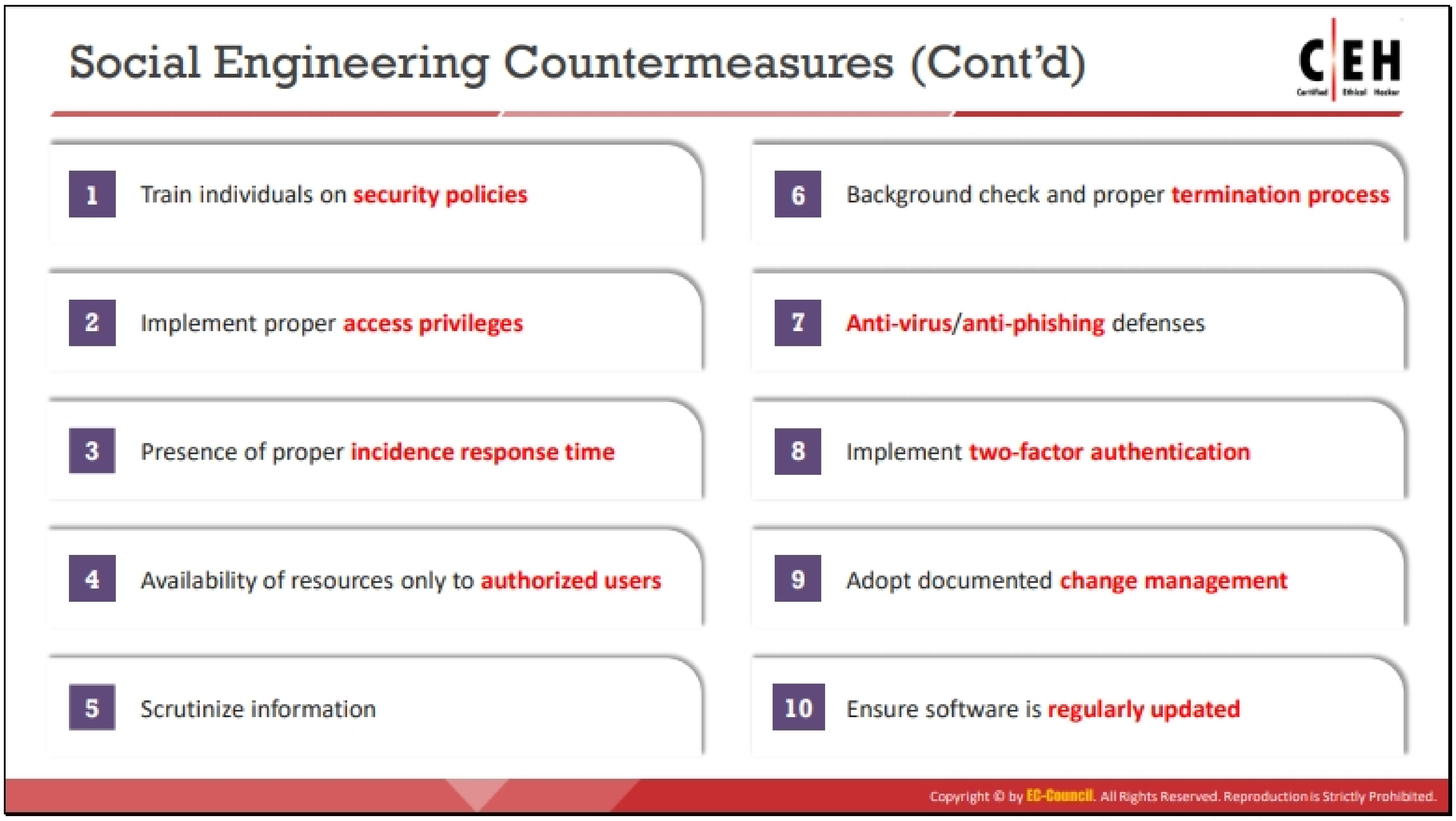
- Periodic password changes
- Avoiding guessable passwords
- Account blocking after failed attempts
- Increasing length and complexity of passwords
- Improving secrecy of passwords

Physical Security Policies

- Identification of employees by issuing ID cards, uniforms, etc.
- Escorting visitors
- Restricting access to work areas
- Proper shredding of useless documents
- Employing security personnel

Defense Strategy

- Social engineering campaign
- Gap analysis
- Remediation strategies



Social Engineering Countermeasures (Cont'd)

1. Train individuals on **security policies**
2. Implement proper **access privileges**
3. Presence of proper **incidence response time**
4. Availability of resources only to **authorized users**
5. Scrutinize information
6. Background check and proper **termination process**
7. **Anti-virus**/**anti-phishing** defenses
8. Implement **two-factor authentication**
9. Adopt documented **change management**
10. Ensure software is **regularly updated**

Social Engineering Countermeasures

Attackers implement social engineering techniques to trick people into revealing organizations' confidential information. They use social engineering to perform fraud, identity theft, industrial espionage, and other disreputable behaviors. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough.

To be truly effective, an organization should:

- Disseminate policies among employees and provide proper education and training. Specialized training benefits employees in higher-risk positions against social engineering threats.
- Obtain employee signatures on a statement acknowledging that they understand the organization’s policies.
- Define the consequences of policy violations.

The main objectives of social engineering defense strategies are to create user awareness, robust internal network controls, and security policies, plans, and processes.

Official security policies and procedures help employees or users make the right security decisions. They should include the following safeguards:

- **Password Policies**

  Password policies stating the following guidelines help to increase password security:

  - Change passwords regularly.
  - Avoid passwords that are easy to guess. It is possible to guess passwords from answers to social engineering questions such as, “Where were you born?” “What is your favorite movie?” or "What is your pet’s name?"
  - Block user accounts if a user exceeds a certain number of failed attempts to guess a password.
  - Choose long (minimum of 6 – 8 characters) and complex (using various alphanumeric and special characters) passwords.
  - Do not disclose passwords to anyone.

  Password Security policies often include advice on proper password management, for example:

  - Avoid sharing a computer account.
  - Avoid using the same password for different accounts.
  - Avoid storing passwords on media or writing them down on a notepad or sticky note.
  - Avoid communicating passwords over the phone or through email or SMS.
  - Be sure to lock or shut down the computer before stepping away from it.

- **Physical Security Policies**

  Physical security policies address the following areas.

  - Issue identification cards (ID cards), and uniforms, along with other access control measures to the employees of the organization.

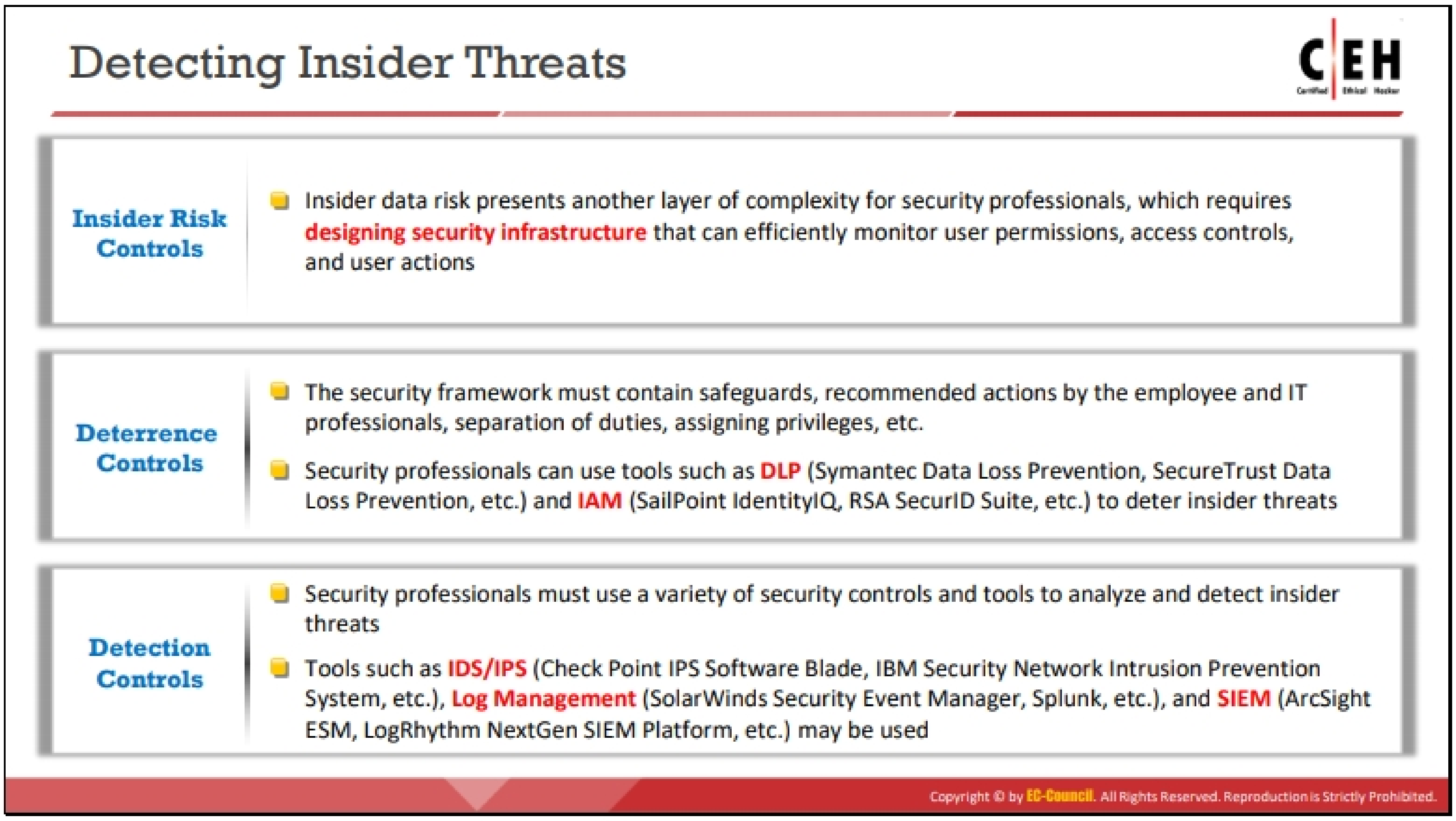
  - Office security or personnel must escort visitors to designated visitor rooms or lounges.
  - Restrict access to certain areas of an organization to prevent unauthorized users from compromising the security of sensitive data.
  - Dispose of old documents that contain valuable information by using equipment such as paper shredders and burn bins. This prevents information gathering by attackers using techniques such as dumpster diving.
  - Employ security personnel in an organization to protect people and property — supplement trained security personnel with alarm systems, surveillance cameras, and other equipment.

- **Defense Strategy**
  - **Social Engineering Campaign**: An organization should conduct numerous social engineering exercises using different techniques on a diverse group of people in order to examine how its employees might react to real social engineering attacks.
  - **Gap Analysis**: Using the information obtained from the social engineering campaign, a gap analysis evaluates the organization based on industry-leading practices, emerging threats, and mitigation strategies.
  - **Remediation Strategies**: Depending upon the result of the evaluation in the gap analysis, organizations develop a detailed remediation plan to mitigate the weaknesses or the loopholes found in the earlier step. The plan focuses mainly on educating and creating awareness among employees based on their roles and identifying and mitigating potential threats to the organization.

Some additional countermeasures against social engineering are as follows:

- **Train Individuals on Security Policies**: An efficient training program consists of basic social engineering concepts and techniques, all security policies, and methods to increase awareness of social engineering.
- **Implement Proper Access Privileges**: There should be administrator, user, and guest accounts with respective levels of authorization.
- **Presence of a Proper Incidence Response Time**: There should be proper guidelines for reacting to a social engineering attempt.
- **Availability of Resources Only to Authorized Users**: Make sure sensitive information is secured and that resources are only accessed by authorized users
- **Scrutinize Information**: Categorize the information as top secret, proprietary, for internal use only, and for public use, or use other categories.
- **Perform a Background Check and Proper Termination Process**: Insiders with a criminal background and terminated employees are easy targets for procuring information.
- **Anti-Virus and Anti-Phishing Defenses**: Use multiple layers of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks.

- **Implement Two-Factor Authentication**: Instead of fixed passwords, use two-factor authentication for high-risk network services such as VPNs and modem pools. In the two-factor authentication (TFA) approach, the user must present two different forms of proof of identity. If an attacker is trying to break into a user account, then they need to break both forms of user identity, which is more difficult to do. Hence, TFA is a defense-in-depth security mechanism and part of the multifactor authentication family. The two pieces of evidence that a user provides could include a physical token such as a card, and is typically something the person can remember without much effort, such as a security code, PIN, or password.
- **Adopt Documented Change Management**: A documented change-management process is more secure than the ad-hoc process.
- **Ensure a Regular Update of Software**: Organizations should ensure that the system and software are regularly patched and updated as the attackers exploit unpatched and out-of-date software to obtain useful information to launch an attack.



Detecting Insider Threats

Insider Risk Controls

- Insider data risk presents another layer of complexity for security professionals, which requires **designing security infrastructure** that can efficiently monitor user permissions, access controls, and user actions

Deterrence Controls

- The security framework must contain safeguards, recommended actions by the employee and IT professionals, separation of duties, assigning privileges, etc.
- Security professionals can use tools such as **DLP** (Symantec Data Loss Prevention, SecureTrust Data Loss Prevention, etc.) and **IAM** (SailPoint IdentityIQ, RSA SecurID Suite, etc.) to deter insider threats

Detection Controls

- Security professionals must use a variety of security controls and tools to analyze and detect insider threats
- Tools such as **IDS/IPS** (Check Point IPS Software Blade, IBM Security Network Intrusion Prevention System, etc.), **Log Management** (SolarWinds Security Event Manager, Splunk, etc.), and **SIEM** (ArcSight ESM, LogRhythm NextGen SIEM Platform, etc.) may be used

Detecting Insider Threats

Most data attacks come from insiders, which only makes them more difficult to prevent or detect. Insiders are mostly aware of the security loopholes of the organization, and they exploit them to steal confidential information. It is essential to carefully handle insider threats as they are difficult to thwart and may incur huge financial losses and business interruptions. Some of the methods to detect insider threats are given below:

- **Insider Risk Controls**

  Insider data risk presents another layer of complexity for security professionals. It requires designing security infrastructure in such a way that user permissions, access controls, and user actions are monitored efficiently.

- **Deterrence Controls**

  The organization's security framework must contain safeguards, follow recommended actions of the employee and IT professionals, provide a separation of duties, and assign privileges. These security controls eliminate or minimize the security risks to the organization's critical assets.

  The deterrence controls that the security professionals must have in place to deter insider threats are DLP (Data Loss Prevention) tools, and Identity and Access Management (IAM) tools.

Some of the deterrence controls are:

- DLP Tools:
  - Symantec Data Loss Prevention (*https://www.symantec.com*)
  - SecureTrust Data Loss Prevention (*https://securetrust.com*)
  - Check Point Data Loss Prevention (*https://www.checkpoint.com*)
- IAM Tools:
  - SailPoint IdentityIQ (*https://www.sailpoint.com*)
  - RSA SecurID Suite (*https://www.rsa.com*)
  - Core Access Assurance Suite (*https://www.coresecurity.com*)

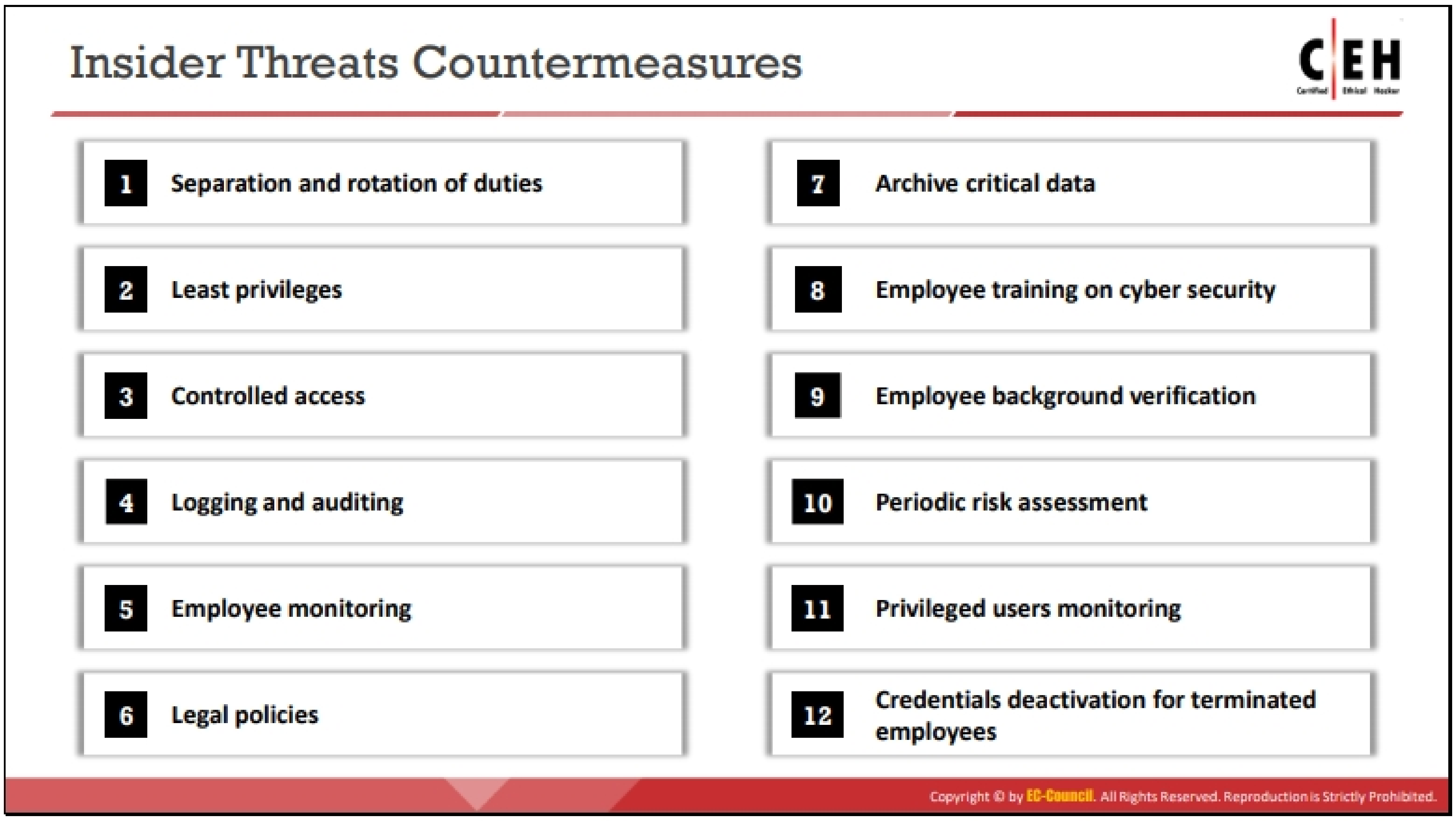
- **Detection Controls**

Security professionals must use a variety of security controls and tools to analyze and detect insider threats in organizations.

The detection controls that the security professionals must have in place to detect insider threats are IDS/IPS (Intrusion detection and prevention systems), log management systems, and Security Information and Event Management (SIEM) tools.

Some of the detection controls are:

- IDS/IPS Tools
  - Check Point IPS Software Blade (*https://www.checkpoint.com*)
  - IBM Security Network Intrusion Prevention System (*https://www.ibm.com*)
  - AlienVault Unified Security Management (*https://www.alienvault.com*)
- Log Management Tools
  - SolarWinds Security Event Manager (*https://www.solarwinds.com*)
  - Splunk (*https://www.splunk.com*)
  - Loggly (*https://www.loggly.com*)
- SIEM Tools
  - ArcSight ESM (*https://www.microfocus.com*)
  - LogRhythm NextGen SIEM Platform (*https://logrhythm.com*)
  - SolarWinds Log & Event Manager(*https://www.solarwinds.com*)



Insider Threats Countermeasures

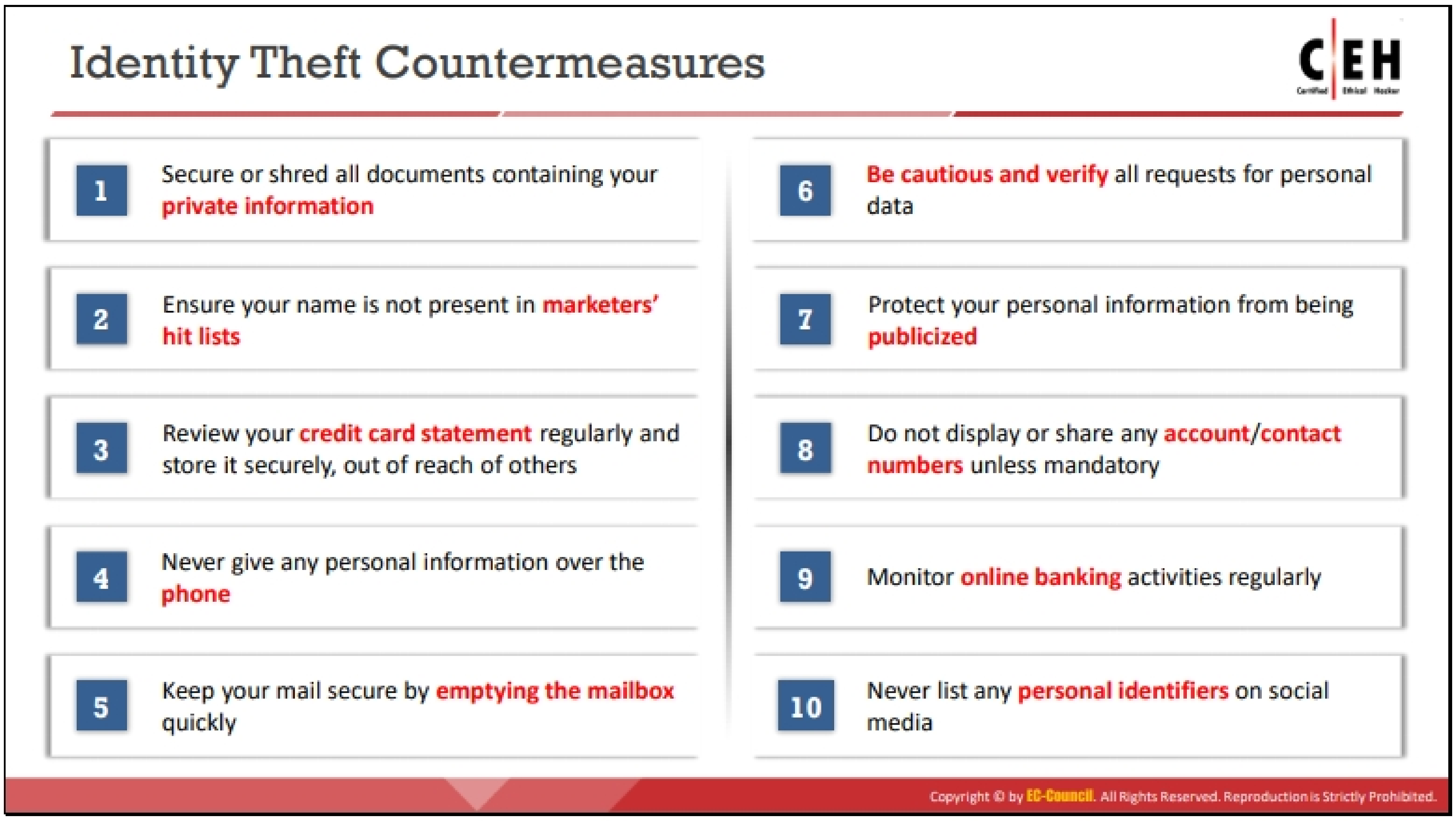
1 Separation and rotation of duties
2 Least privileges
3 Controlled access
4 Logging and auditing
5 Employee monitoring
6 Legal policies
7 Archive critical data
8 Employee training on cyber security
9 Employee background verification
10 Periodic risk assessment
11 Privileged users monitoring
12 Credentials deactivation for terminated employees

Insider Threats Countermeasures

There are safety measures that help an organization to prevent or minimize insider threats:

- **Separation and rotation of duties**: Divide responsibilities among multiple employees to restrict the amount of power or influence held by any individual. This helps to avoid fraud, abuse, and conflict of interest and facilitates the detection of control failures (including bypassing security controls and information theft). Rotation of duties at random intervals helps an organization to deter fraud or the abuse of privileges.
- **Least privileges**: Provide users with only enough access privilege to allow them to perform their assigned tasks. This helps maintain information security.
- **Controlled access**: Access controls in various parts of an organization restrict unauthorized users from gaining access to critical assets and resources.
- **Logging and auditing**: Perform logging and auditing periodically to check for misuse of company resources.
- **Employee monitoring**: Use employee monitoring software that records all user sessions, and that can be reviewed by security professionals.
- **Legal policies**: Enforce legal policies to prevent employees from misusing the organization’s resources and sensitive data theft.
- **Archive critical data**: Maintain a record of the organization’s critical data in the form of archives to be used as backup resources, if needed.
- **Employee training on cybersecurity**: Train employees on how to protect their credentials and the company’s confidential data from attack. They will be able to identify social engineering attempts and take proper mitigations and reporting steps.

- **Employee background verification**: Ensure thorough background checks of all employees before hiring them by using Google search and social networking sites and consulting previous employers.
- **Periodic risk assessment**: Perform a periodic risk assessment on critical assets to identify vulnerabilities and implement protection strategies against both insider and outsider threats.
- **Privileged users monitoring**: Implement additional monitoring mechanisms for system administrators and privileged users as these accounts can be used to can deploy malicious code or logic bomb on the system or network.
- **Credentials deactivation for terminated employees**: Disable all the employee's access profiles to the physical locations, networks, systems, applications, and data immediately after termination.
- **Periodic risk assessments**: Perform periodic risk assessments on all the organization's critical assets then develop and maintain a risk management strategy to secure those assets from both insiders and outsiders.
- **Layered defense**: Implement multiple layers of defense to prevent and protect critical assets from remote attacks originated from insiders. Develop appropriate remote access policies and procedures to thwart such attacks.
- **Physical security**: Build a professional security team that monitors the physical security of the organization.
- **Surveillance**: Install video cameras to monitor all critical assets. Install and enable screen-capturing software on all critical servers.



Identity Theft Countermeasures

1. Secure or shred all documents containing your **private information**
2. Ensure your name is not present in **marketers' hit lists**
3. Review your **credit card statement** regularly and store it securely, out of reach of others
4. Never give any personal information over the **phone**
5. Keep your mail secure by **emptying the mailbox** quickly
6. **Be cautious and verify** all requests for personal data
7. Protect your personal information from being **publicized**
8. Do not display or share any **account**/**contact numbers** unless mandatory
9. Monitor **online banking** activities regularly
10. Never list any **personal identifiers** on social media

Identity Theft Countermeasures

Identity theft occurs when someone uses personal information (such as a name, social security number, date of birth, mother's maiden name, or address) in a malicious way, such as for credit card or loan services, or even rentals and mortgages, without the person's knowledge or permission.

Listed below are countermeasures that, on implementation, will reduce the chances of identity theft:

- Secure or shred all documents containing private information
- Ensure your name is not present on the marketers' hit lists
- Review credit card reports regularly
- Never give any personal information over the phone
- To keep mail secure, empty the mailbox quickly
- Suspect and verify all requests for personal data
- Protect personal information from being publicized
- Do not display account or contact numbers unless mandatory
- Monitor online banking activities regularly
- Never list any personal identifiers on social media websites such as your father's name, pet's name, address, or city of birth.
- Enable two-factor authentication on all online accounts
- Never use public Wi-Fi for sharing or accessing sensitive information

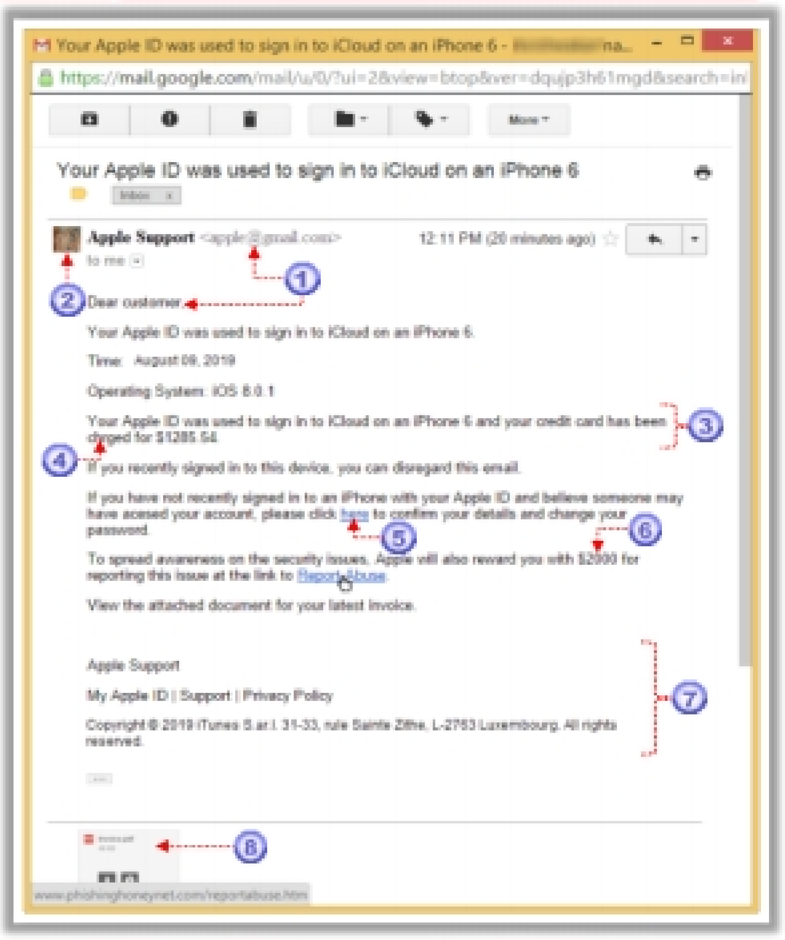
- Install host security tools such as a firewall and anti-virus on your personal computer

Some additional countermeasures against identity theft are as follows:

- To keep mail secure, empty your mailbox quickly and do not reply to unsolicited email requests asking for personal information.
- Shred credit card offers and “convenience checks” that are not useful.
- Do not store any financial information on the system and use strong passwords for all financial accounts.
- Check telephone and cell phone bills for calls you did not make.
- Keep your Social Security card, passport, license, and other valuable personal information hidden and secured.
- Read website privacy policies.
- Be cautious before clicking on a link provided in an email or instant message.

How to Detect Phishing Emails?

1. Appears to be from a **bank**, **company**, or **social networking site**, and has a **generic greeting**
2. Appears to be from a person listed in your **email address book**
3. Gives a sense of **urgency** or a **veiled threat**
4. May contain **grammatical/spelling mistakes**
5. Includes links to **spoofed websites**
6. May contain **offers that seem to be too good to be true**
7. Includes **official-looking logos** and other information taken from legitimate websites
8. May contain a **malicious attachment**


Your Apple ID was used to sign in to iCloud on an iPhone 6 - [redacted]na...
https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=dqujp3h61mgd&search=in
More
Inbox
①
②
③
④
⑤
⑥
⑦
⑧
www.phishinghoneynet.com/reportabuse.htm

Your Apple ID was used to sign in to iCloud on an iPhone 6

Apple Support <apple@gmail.com> 12:11 PM (20 minutes ago)
to me

Dear customer,

Your Apple ID was used to sign in to iCloud on an iPhone 6.

Time: August 09, 2019

Operating System: iOS 8.0.1

Your Apple ID was used to sign in to iCloud on an iPhone 6 and your credit card has been cdrged for $1285.54

If you recently signed in to this device, you can disregard this email.

If you have not recently signed in to an iPhone with your Apple ID and believe someone may have acesed your account, please click here to confirm your details and change your password.

To spread awareness on the security issues, Apple will also reward you with $2000 for reporting this issue at the link to Report Abuse.

View the attached document for your latest invoice.

Apple Support

My Apple ID | Support | Privacy Policy

Copyright © 2019 iTunes S.a.r.l. 31-33, rule Sainte Zithe, L-2763 Luxembourg. All rights reserved.

How to Detect Phishing Emails?

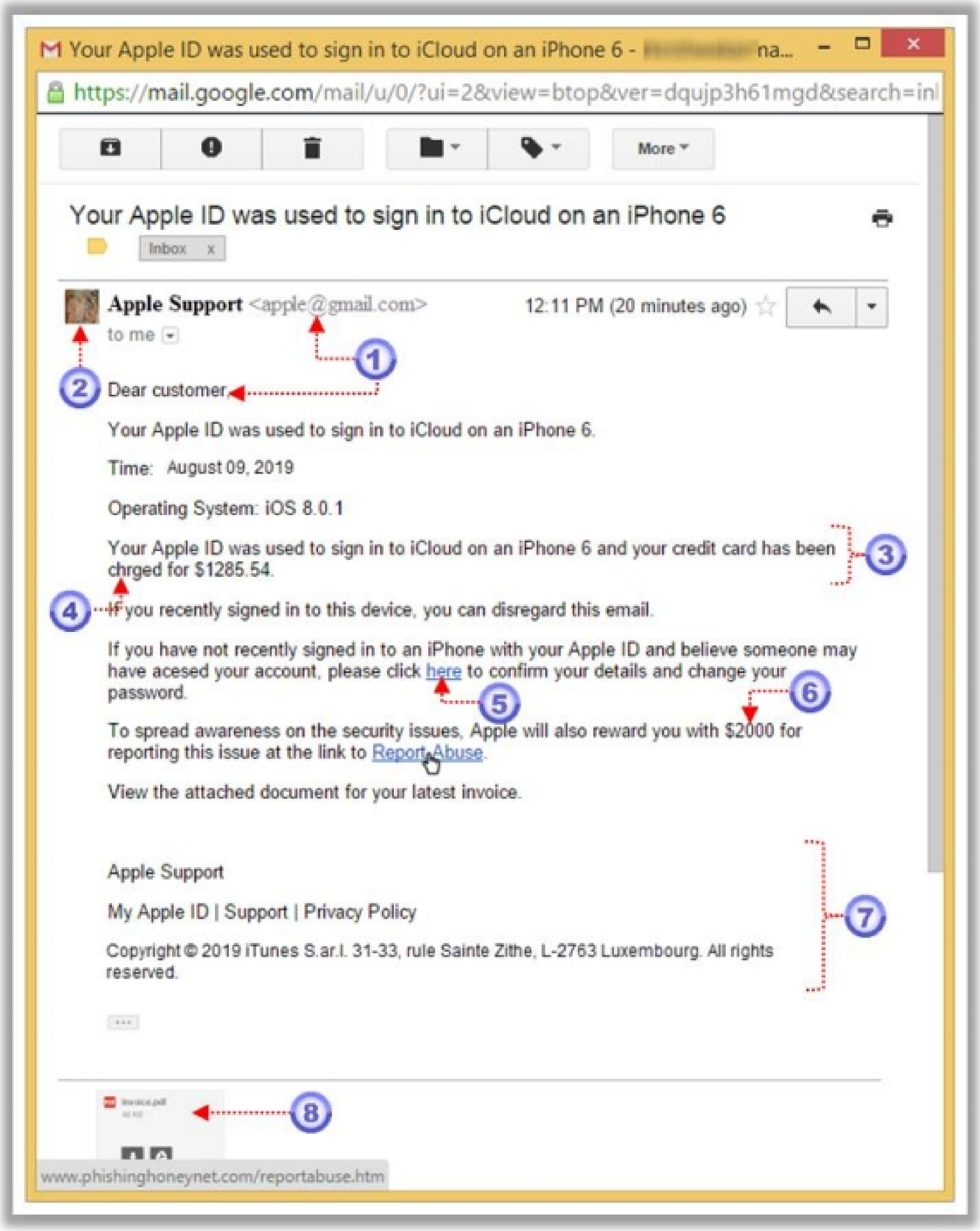
To detect phishing emails, first, hover your mouse pointer over the name in the "**From**" column. Doing so will show whether the original domain name is linked to the sender's name; if it is not, then it could be a phishing email. For example, an email from Gmail.com should probably display it's "**From**" domain as "**gmail.com**."

Check to see if the email provides a URL and prompts the user to click on it. If so, ensure that the link is legitimate by hovering the mouse pointer over it (to display the link's URL) and ensure it uses encryption (https://). To be on the safe side, always open a new window and visit the site by typing it in directly instead of clicking on the link provided in the email.

Do not provide any information to the suspicious website, as it will likely link directly to the attacker.

A few other indicators of phishing emails:

- It seems to be from a bank, company, or social networking site and has a generic greeting
- It seems to be from a person listed in your email address book
- It has an urgent tone or makes a veiled threat
- It may contain grammatical or spelling mistakes
- It includes links to spoofed websites
- It may contain offers that seem to be too good to be true
- It includes official-looking logos and other information taken from legitimate websites
- It may contain a malicious attachment


Your Apple ID was used to sign in to iCloud on an iPhone 6 - [redacted]na...
https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=dqujp3h61mgd&search=inl
More
Inbox x
①
②
③
④
⑤
⑥
⑦
⑧
invoice.pdf
www.phishinghoneynet.com/reportabuse.htm

Your Apple ID was used to sign in to iCloud on an iPhone 6

Apple Support <apple@gmail.com>
to me

12:11 PM (20 minutes ago)

Dear customer,

Your Apple ID was used to sign in to iCloud on an iPhone 6.

Time: August 09, 2019

Operating System: iOS 8.0.1

Your Apple ID was used to sign in to iCloud on an iPhone 6 and your credit card has been chrged for $1285.54.

If you recently signed in to this device, you can disregard this email.

If you have not recently signed in to an iPhone with your Apple ID and believe someone may have acesed your account, please click here to confirm your details and change your password.

To spread awareness on the security issues, Apple will also reward you with $2000 for reporting this issue at the link to Report Abuse.

View the attached document for your latest invoice.

Apple Support

My Apple ID | Support | Privacy Policy

Copyright © 2019 iTunes S.ar.l. 31-33, rule Sainte Zithe, L-2763 Luxembourg. All rights reserved.

Figure 9.15: Screenshot Showing an Email with Indications of Phishing

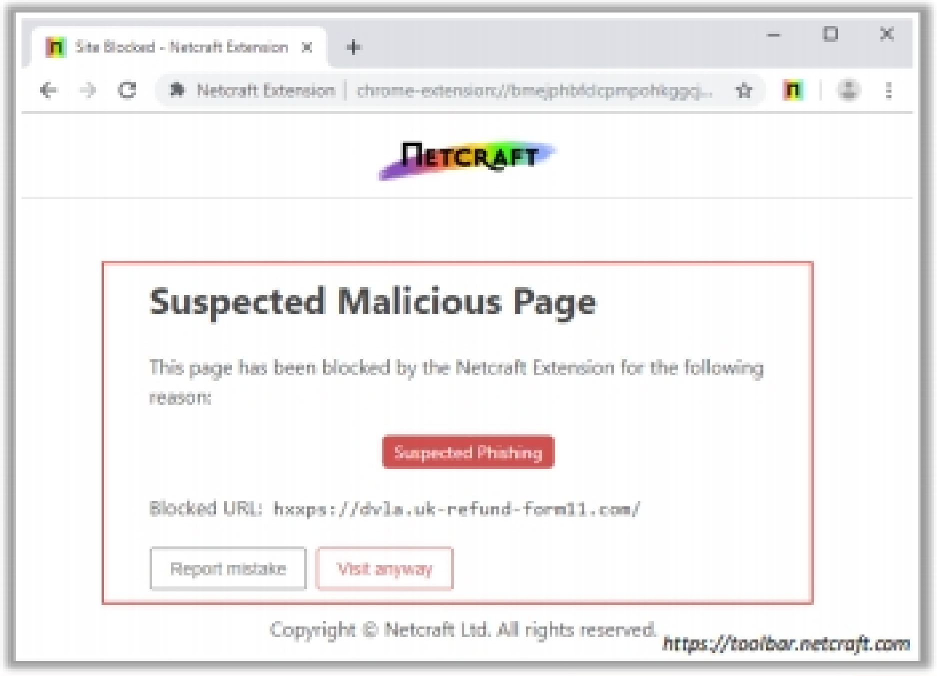
Anti-Phishing Toolbar

Netcraft

- The Netcraft **anti-phishing community** is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks

Phish Tank

- PhishTank is a collaborative clearing house for data and information about **phishing** on the Internet
- It provides an **open API** for developers and researchers to integrate **anti-phishing data** into their apps


Site Blocked - Netcraft Extension
Netcraft Extension | chrome-extension://bmejphbfdcpmpohkggq...
NETCRAFT
Suspected Phishing
Report mistake
Visit anyway

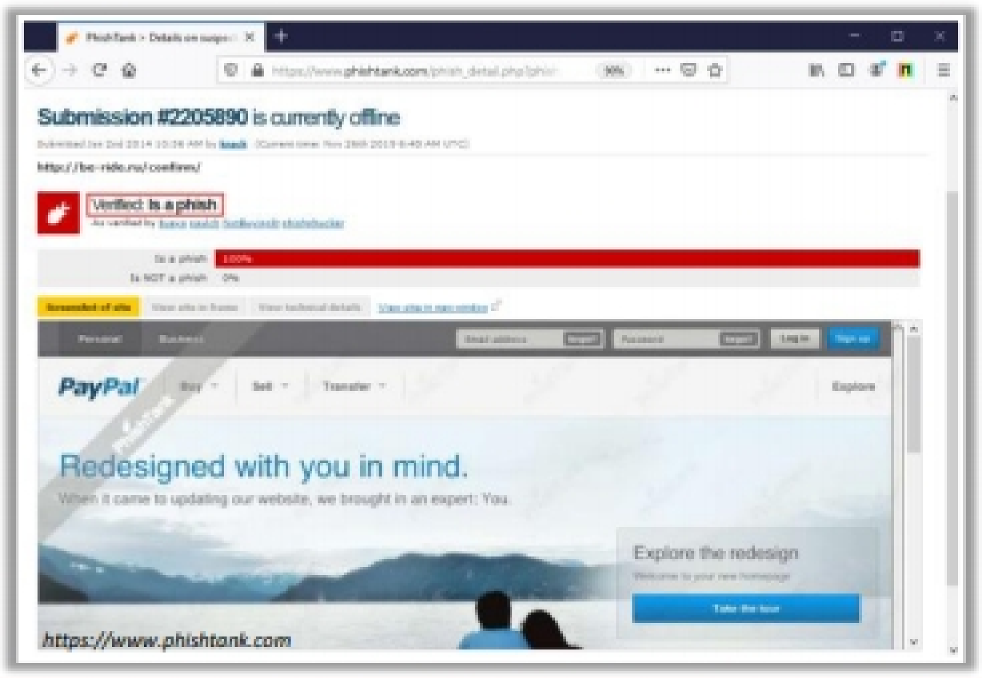
Suspected Malicious Page

This page has been blocked by the Netcraft Extension for the following reason:

Blocked URL: `hxxps://dvla.uk-refund-form11.com/`

Copyright © Netcraft Ltd. All rights reserved.

https://toolbar.netcraft.com


PhishTank > Details on suspe...
https://www.phishtank.com/phish_detail.php?phis
PayPal
Explore the redesign

Submission #2205890 is currently offline

http://be-ride.ru/confirm/

Verified: Is a phish

Is a phish 100%

Is NOT a phish 0%

Redesigned with you in mind.

When it came to updating our website, we brought in an expert: You.

https://www.phishtank.com

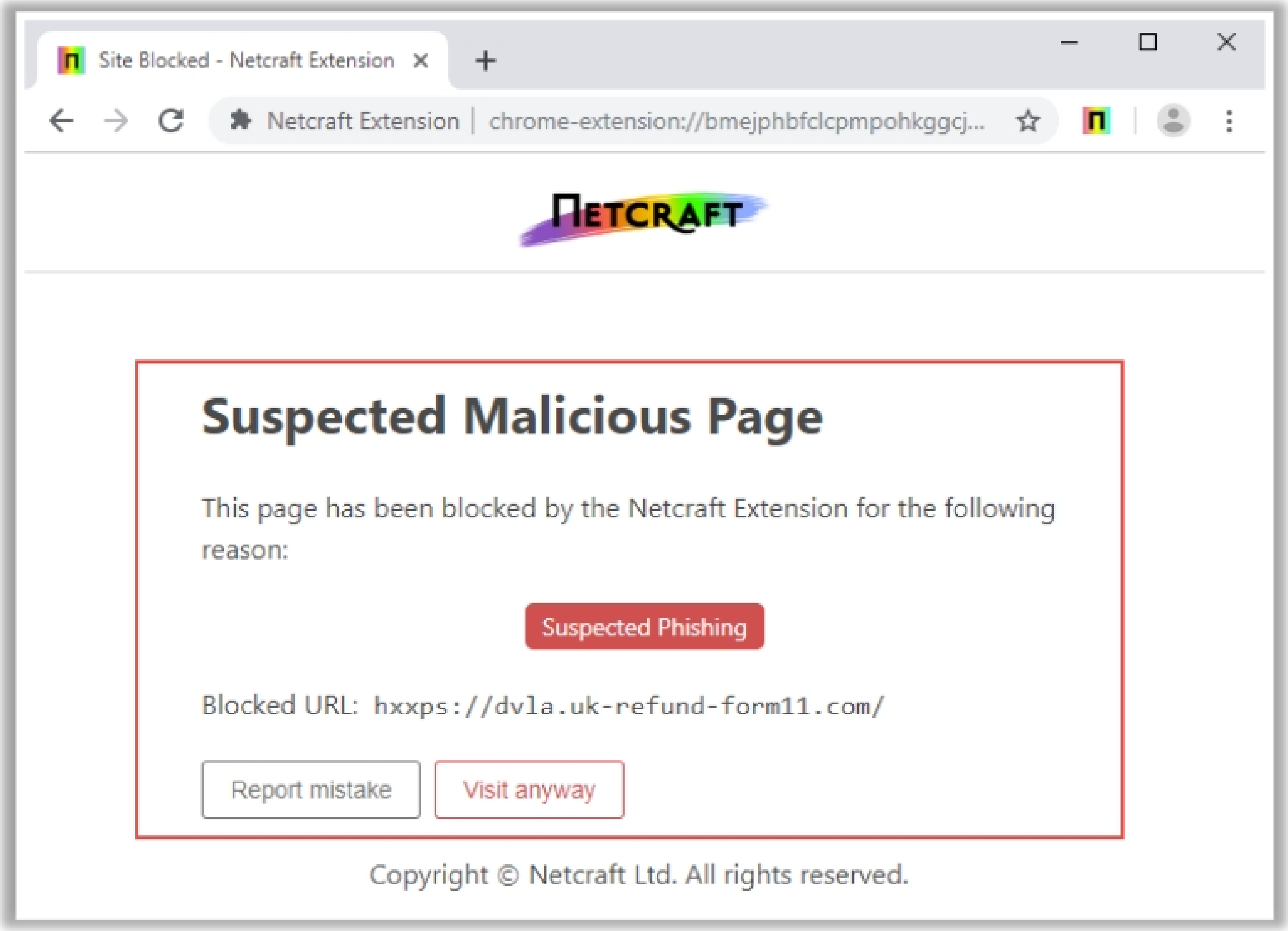
Anti-Phishing Toolbar

- **Netcraft**

  Source: *https://toolbar.netcraft.com*

  The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Toolbar provides updated information about sites that users visit regularly and blocks dangerous sites. The toolbar provides a wealth of information about popular websites. This information will help to make an informed choice about the integrity of those sites.

  As shown in the screenshot, Netcraft protects individuals and organizations from phishing attacks and fraudsters.


Site Blocked - Netcraft Extension
Netcraft Extension | chrome-extension://bmejphbfclcpmpohkggcj...
NETCRAFT

Suspected Malicious Page

This page has been blocked by the Netcraft Extension for the following reason:

Suspected Phishing

Blocked URL: `hxxps://dvla.uk-refund-form11.com/`

Report mistake
Visit anyway

Copyright © Netcraft Ltd. All rights reserved.

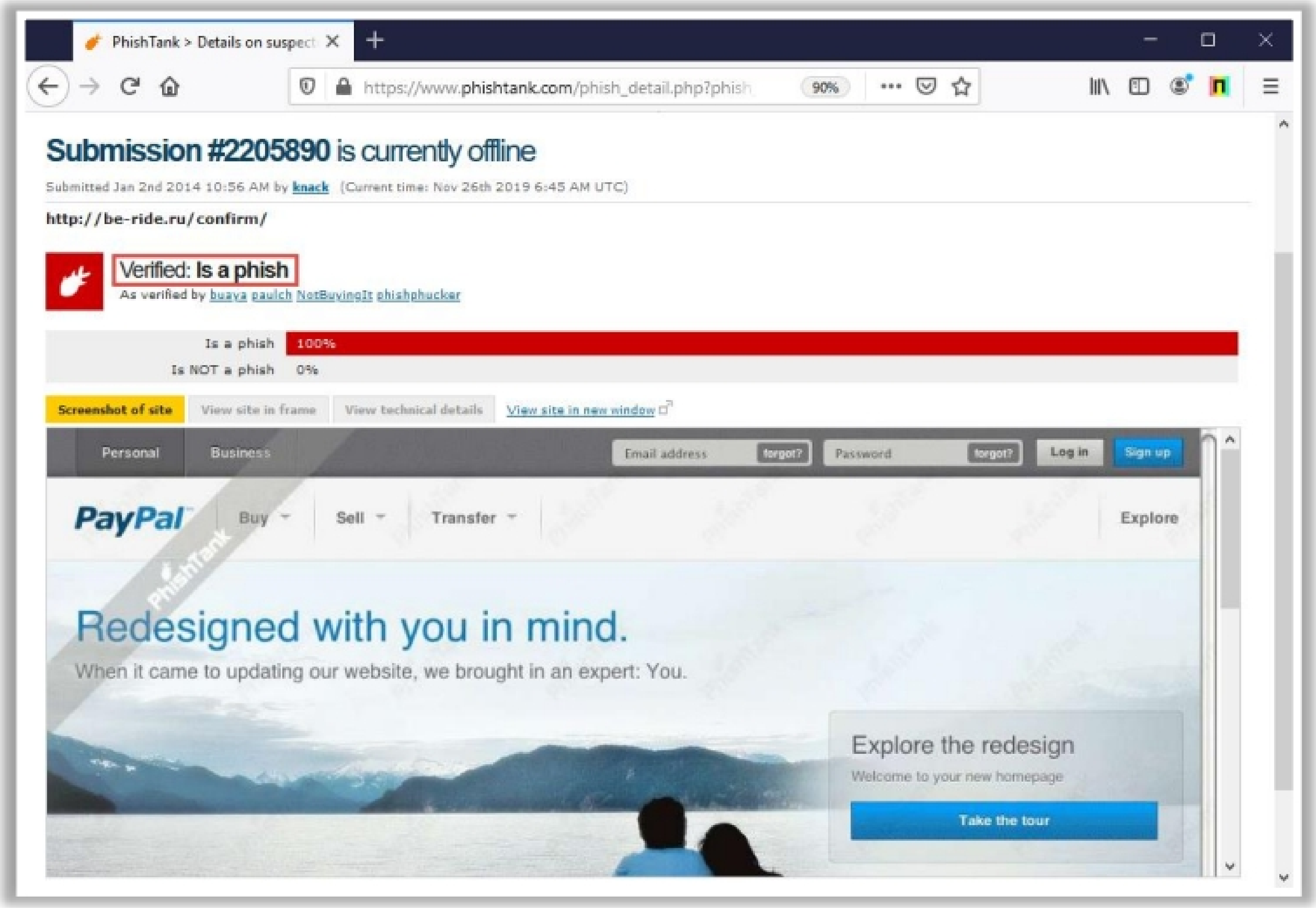
Figure 9.16: Screenshot of Netcraft

- **PhishTank**

  Source: *https://phishtank.com*

  PhishTank is a collaborative clearinghouse for data and information about phishing on the Internet. It provides an open API for developers and researchers to integrate anti-phishing data into their applications.

  As shown in the screenshot, security professionals can use PhishTank to check whether a malicious URL is a phishing site or not.



Submission #2205890 is currently offline

Submitted Jan 2nd 2014 10:56 AM by knack (Current time: Nov 26th 2019 6:45 AM UTC)

http://be-ride.ru/confirm/

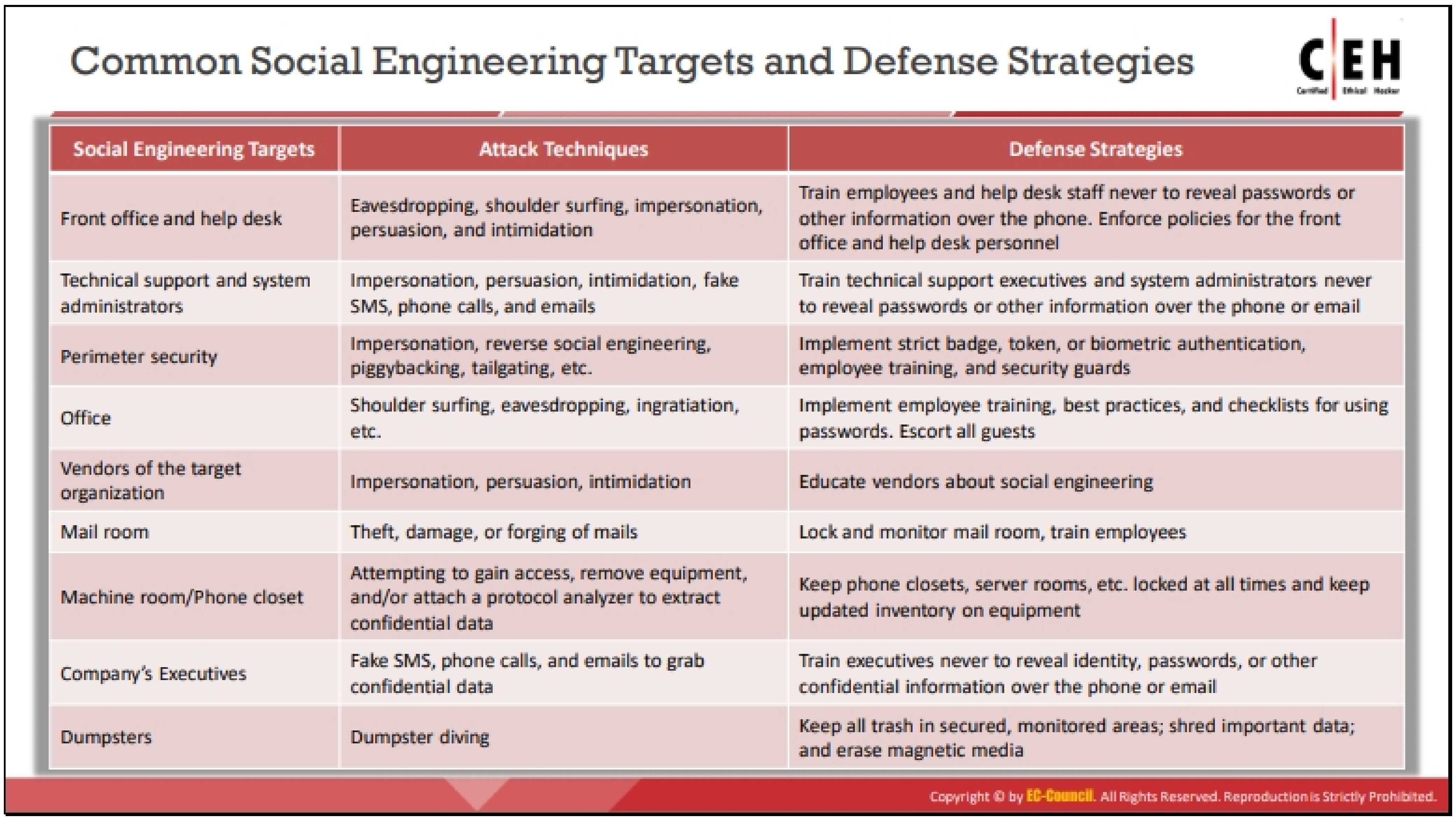
Verified: Is a phish

As verified by buaya paulch NotBuyingIt phishphucker

Is a phish	100%
Is NOT a phish	0%

PhishTank > Details on suspect
https://www.phishtank.com/phish_detail.php?phish
90%
Screenshot of site
View site in frame
View technical details
View site in new window
Personal
Business
Email address
forgot?
Password
forgot?
Log in
Sign up
PayPal
Buy
Sell
Transfer
Explore
PhishTank
Redesigned with you in mind.
When it came to updating our website, we brought in an expert: You.
Explore the redesign
Welcome to your new homepage
Take the tour

Figure 9.17: Screenshot of PhishTank



Common Social Engineering Targets and Defense Strategies

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees and help desk staff never to reveal passwords or other information over the phone. Enforce policies for the front office and help desk personnel
Technical support and system administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators never to reveal passwords or other information over the phone or email
Perimeter security	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token, or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, ingratiation, etc.	Implement employee training, best practices, and checklists for using passwords. Escort all guests
Vendors of the target organization	Impersonation, persuasion, intimidation	Educate vendors about social engineering
Mail room	Theft, damage, or forging of mails	Lock and monitor mail room, train employees
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to extract confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Company's Executives	Fake SMS, phone calls, and emails to grab confidential data	Train executives never to reveal identity, passwords, or other confidential information over the phone or email
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas; shred important data; and erase magnetic media

Common Social Engineering Targets and Defense Strategies

Attackers implement various social engineering techniques to trick people into providing sensitive information about their organizations, thus helping attackers to launch malicious activities. These techniques are used on privileged individuals or those who deal with important information.

Below table shows common social engineering targets, various social engineering techniques that attackers use, and the defense strategies to counter these attacks.

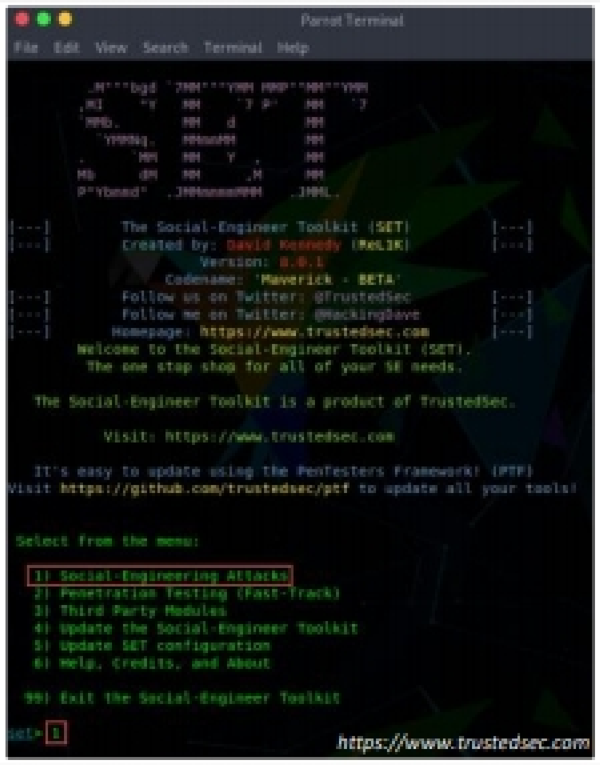
Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees and help desk staff never to reveal passwords or other information over the phone. Enforce policies for the front office and help desk personnel
Technical support and system administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators never to reveal passwords or other information over the phone or email
Perimeter security	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token, or biometric authentication, employee training, and security guards

Office	Shoulder surfing, eavesdropping, and ingratiation	Implement employee training, best practices, and checklists for using passwords. Escort all guests
Vendors of the target organization	Impersonation, persuasion, and intimidation	Educate vendors about social engineering.
Mail room	Theft, damage, or forging of mails	Lock and monitor the mailroom, train employees
Machine room and Phone closet	Attempting to gain access, remove equipment, or attach a protocol analyzer to extract confidential data	Keep phone closets, server rooms, and other spaces locked at all times and keep an updated inventory of equipment
Company's Executives	Fake SMS, phone calls, and emails designed to grab confidential data	Train executives never to reveal identity, passwords, or other confidential information over the phone or email
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas; shred important data; and erase magnetic media

Table 9.1: Common social engineering targets and defense strategies

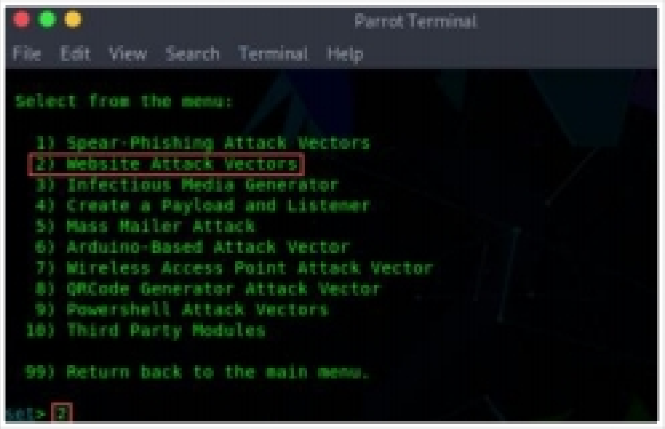
Social Engineering Tools: Social Engineering Toolkit (SET)

- The Social-Engineer Toolkit (SET) is an open-source **Python-driven tool** aimed at penetration testing around social engineering



```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                  Version: 8.0.1
              Codename: 'Maverick - BETA'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

https://www.trustedsec.com



```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

SpeedPhish Framework (SPF)
https://github.com

Gophish
https://getgophish.com

King Phisher
https://github.com

LUCY
https://www.lucysecurity.com

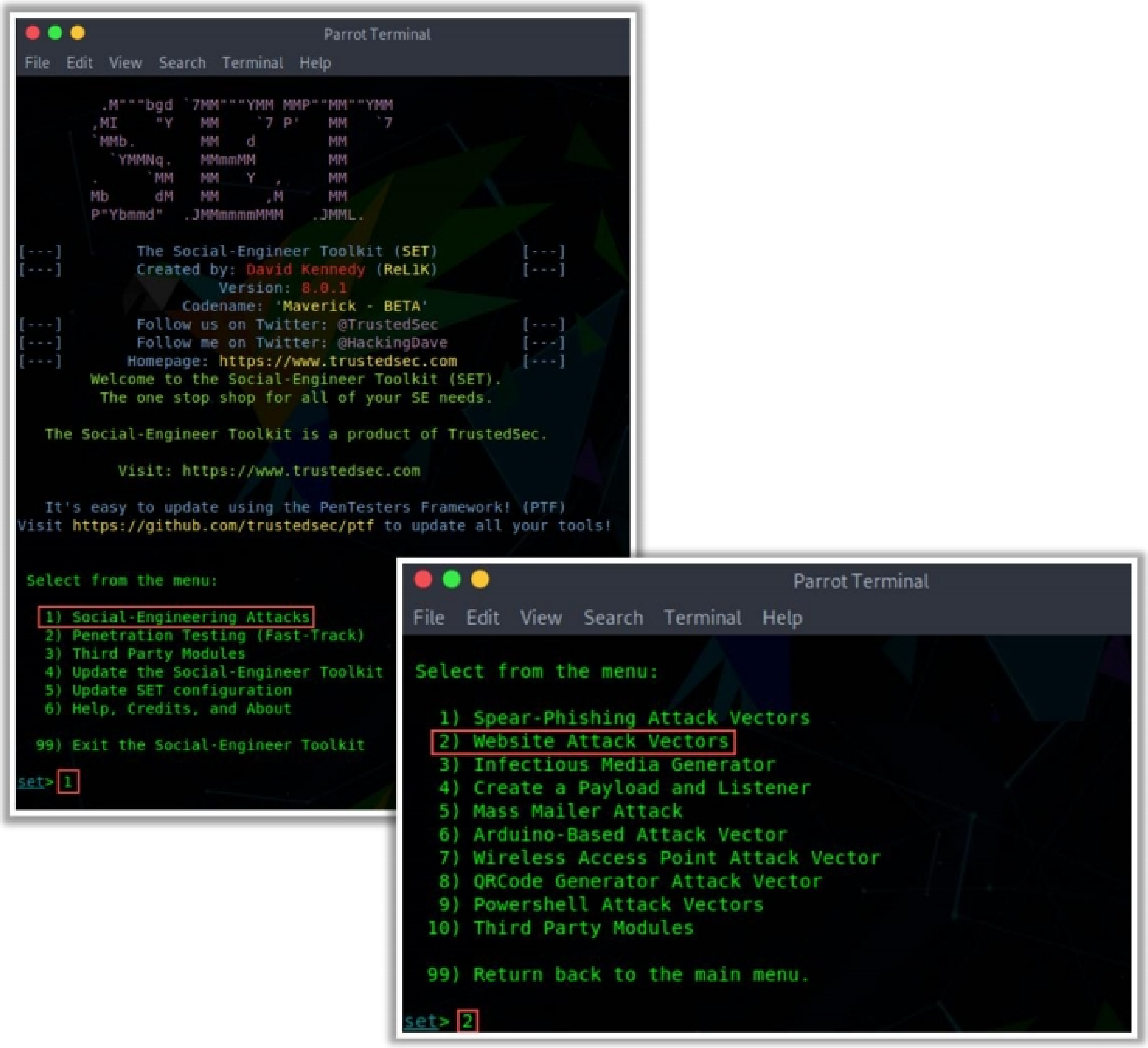
MSI Simple Phish
https://microsolved.com

Social Engineering Tools

- **Social Engineering Toolkit (SET)**

  Source: *https://www.trustedsec.com*

  The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. It is a generic exploit designed to perform advanced attacks against human elements to compromise a target and make them offer sensitive information. SET categorizes attacks such as email, web, and USB attacks according to the attack vector used to trick humans. The toolkit attacks human weakness, exploiting the trusting, fearful, greedy, and the helpful nature of humans.



```
         .M"""bgd `7MM"""YMM MMP""MM""YMM
        ,MI    "Y   MM    `7 P'   MM   `7
        `MMb.       MM   d        MM
          `YMMNq.   MMmmMM        MM
        .     `MM   MM   Y  ,     MM
        Mb     dM   MM     ,M     MM
        P"Ybmmd"  .JMMmmmmMMM   .JMML.

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.1
                  Codename: 'Maverick - BETA'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

Figure 9.18: Screenshot of SET showing menu and attack options

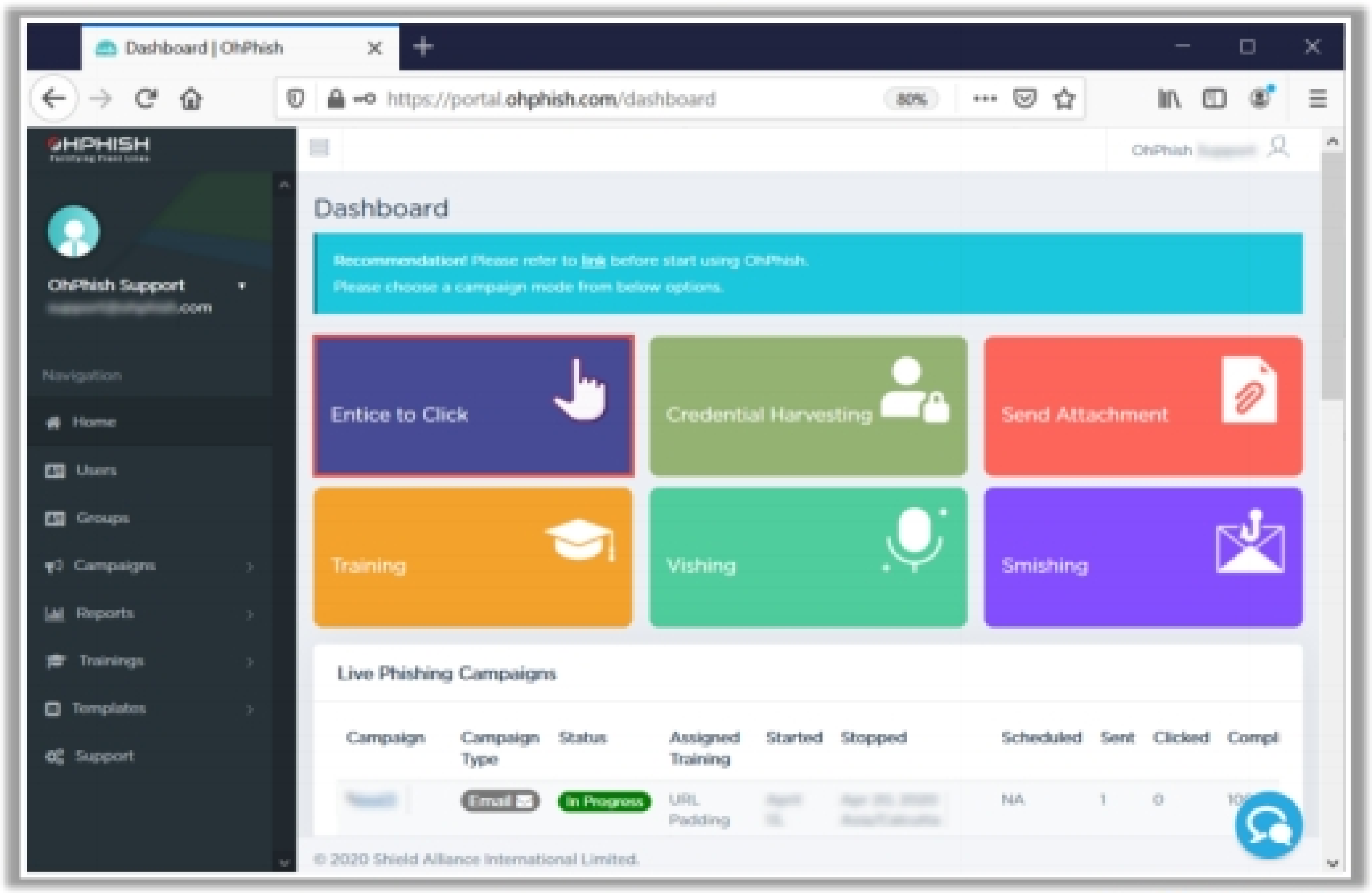
Some social engineering tools are listed below:

- SpeedPhish Framework (SPF) (*https://github.com*)
- Gophish (*https://getgophish.com*)
- King Phisher (*https://github.com*)
- LUCY (*https://www.lucysecurity.com*)
- MSI Simple Phish (*https://microsolved.com*)

Audit Organization's Security for Phishing Attacks using OhPhish

- OhPhish is a web-based portal to **test employees' susceptibility to social engineering attacks**
- OhPhish is a phishing simulation tool that provides the organization with a **platform to launch phishing simulation campaigns** on its employees

OHPHISH
Fortifying Front Lines


Dashboard | OhPhish
https://portal.ohphish.com/dashboard
80%
OHPHISH
OhPhish Support
OhPhish Support
Navigation
Home
Users
Groups
Campaigns
Reports
Trainings
Templates
Support
Dashboard
Entice to Click
Credential Harvesting
Send Attachment
Training
Vishing
Smishing
Live Phishing Campaigns
Email
In Progress

Recommendation! Please refer to link before start using OhPhish.
Please choose a campaign mode from below options.

Campaign	Campaign Type	Status	Assigned Training	Started	Stopped	Scheduled	Sent	Clicked	Compl
[redacted]	Email	In Progress	URL Padding	[redacted]	[redacted]	NA	1	0	10

© 2020 Shield Alliance International Limited.

https://ohphish.eccouncil.org

Audit Organization's Security for Phishing Attacks using OhPhish

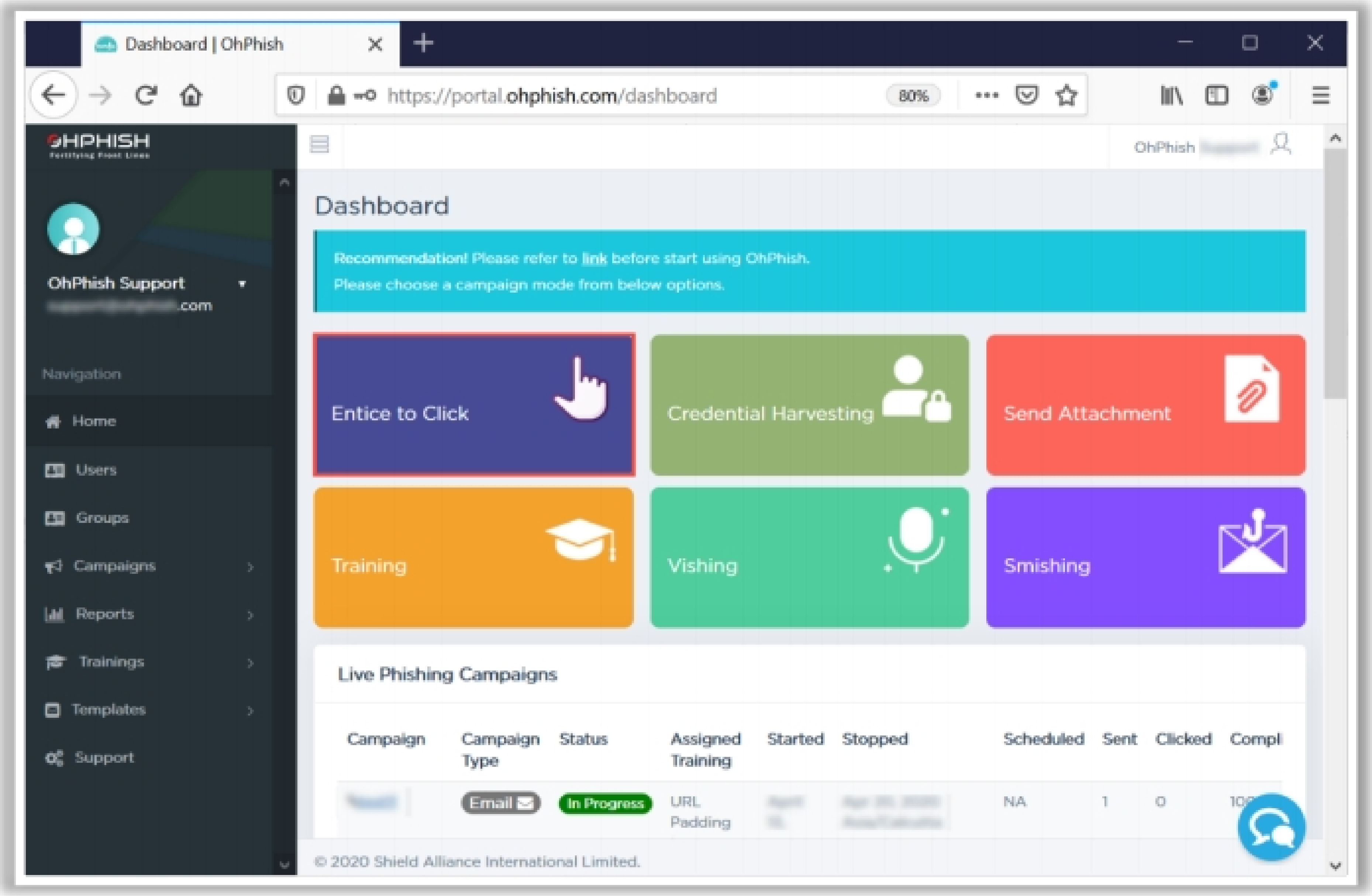
The primary objective of launching phishing campaigns against employees of the client organization is to assess the employees' susceptibility to phishing attacks and help the organization reduce risks that arise when the employees fall prey to phishing attacks sent by cyber-threat actors.

- **OhPhish**

  Source: *https://ohphish.eccouncil.org*

  OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides the organization with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

  OhPhish can be used to audit an organization's security for phishing attacks using various phishing methods such as Entice to Click, Credential Harvesting, Send Attachment, Training, Vishing, and Smishing.

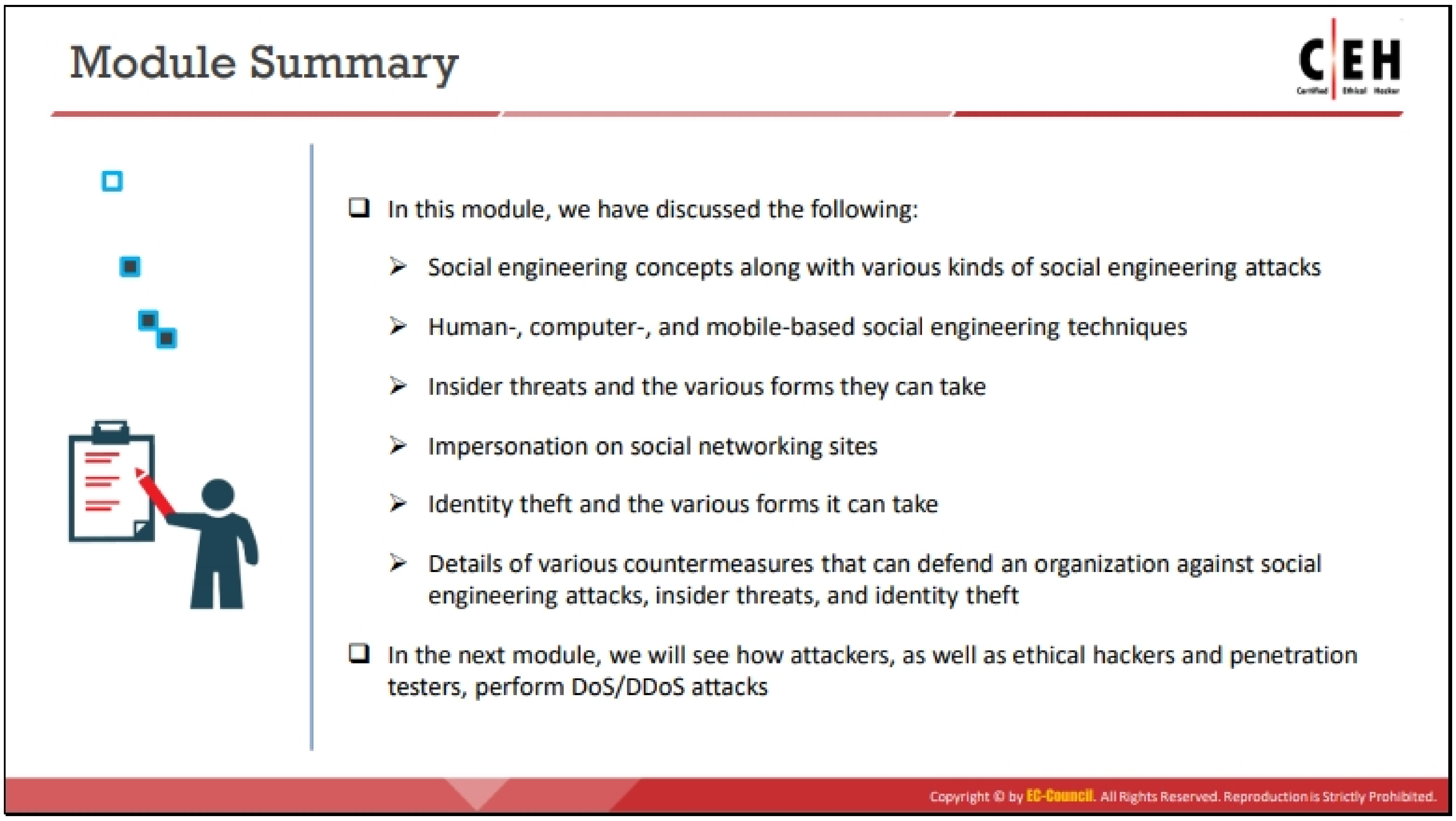

Dashboard | OhPhish
https://portal.ohphish.com/dashboard
80%
OHPHISH
Fortifying Front Lines
OhPhish Support
[redacted].com
OhPhish [redacted]
Navigation
Home
Users
Groups
Campaigns
Reports
Trainings
Templates
Support
Dashboard
Entice to Click
Credential Harvesting
Send Attachment
Training
Vishing
Smishing
© 2020 Shield Alliance International Limited.

Recommendation! Please refer to link before start using OhPhish.
Please choose a campaign mode from below options.

Live Phishing Campaigns

Campaign	Campaign Type	Status	Assigned Training	Started	Stopped	Scheduled	Sent	Clicked	Compl
[redacted]	Email	In Progress	URL Padding	[redacted]	[redacted]	NA	1	0	10

Figure 9.19: Screenshot of OhPhish



Module Summary

- In this module, we have discussed the following:
    - Social engineering concepts along with various kinds of social engineering attacks
    - Human-, computer-, and mobile-based social engineering techniques
    - Insider threats and the various forms they can take
    - Impersonation on social networking sites
    - Identity theft and the various forms it can take
    - Details of various countermeasures that can defend an organization against social engineering attacks, insider threats, and identity theft
- In the next module, we will see how attackers, as well as ethical hackers and penetration testers, perform DoS/DDoS attacks

Module Summary

This module discussed social engineering concepts along with various phases of social engineering attack. It also discussed various human-based, computer-based, and mobile-based social engineering techniques. The module discussed insider threats, including the various types of insider threats. It gave an overview of impersonation on social networking sites. It also discussed identity theft and the types of identity theft. The module ended with a detailed discussion of various signs to watch for and countermeasures to employ in order to defend against social engineering attacks, insider threats, and identity theft.

The next module will show how attackers, as well as ethical hackers and pen testers, perform DoS/DDoS attacks.